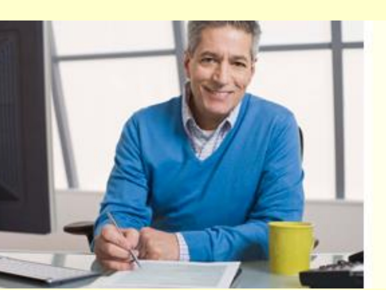
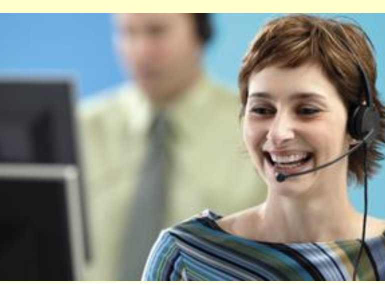
Beratung und Support
Technische Plattform
Support-Netz-Portal



paedML® – stabil und zuverlässig vernetzen

Anleitung

Administrationshandbuch

Stand 06.11.2014

paedML® Linux

Version: 6.0





Impressum

Herausgeber

Landesmedienzentrum Baden-Württemberg (LMZ)
Support-Netz
Rotenbergstraße 111

70190 Stuttgart

Autoren

der Zentralen Expertengruppe Netze (ZEN),
Support-Netz, LMZ

Roland Walter, Michael Salm

Endredaktion

Redaktion Support-Netz

Bildnachweis Titelbilder:

Thinkstock

Weitere Informationen

www.support-netz.de
www.lmz-bw.de

Veröffentlicht: 2014

Inhaltsverzeichnis

Einführung

Vielen Dank, dass Sie sich für die *paedML Linux* entschieden haben. Die Arbeit mit Computern bietet täglich vielfältige Herausforderungen, denen Sie sich als IT-Verantwortlicher Ihrer Schule stellen müssen. Wir hoffen, dass wir mit unserem Produkt dazu beitragen, dass Sie die an Sie gestellten Aufgaben meistern und Spaß an der Arbeit als Netzwerkberater haben.

Die *paedML Linux 6.0* ist eine Neuentwicklung, die im Vergleich zu ihren Vorgängerversionen mit einem komplett neuen Server- und Clientmanagement ausgestattet wurde. *Univention Corporate Server („UCS“* mit der Applikation *UCS@school*) bilden nun die technologische Plattform für die Schul-IT-Komplettlösung. Damit ist die *paedML* hervorragend geeignet, um IT-Infrastrukturen im Schulumfeld bereitzustellen und zu verwalten. Für Lehrkräfte wurde die Anwenderoberfläche neu gestaltet und mit einer intuitiven „*Schulkonsole*“ ausgestattet. Hinzugekommen sind neue Steuerungsfunktionen, die den Lehrkräften noch mehr Sicherheit beim Unterrichten geben (zum Beispiel „Schülercomputer steuern“, „Klassenarbeiten schreiben“, „Internet verwalten“ oder „Drucker moderieren“). Die neue Version ermöglicht deutlich mehr Mobilität beim Lernen, denn Schülerinnen und Schüler können auch mit ihren privaten Geräten im „*Gäste-Netz*“ der Schule arbeiten (*Bring Your Own Device*). Schuleigene Geräte sind im pädagogischen Schulnetz integriert.

Neben den Verbesserungen für den aktiven Unterrichtablauf bringt die *paedML Linux 6.0* auch für Netzwerkbetreuer deutliche Arbeitserleichterungen mit sich: Viele Installationsroutinen wurden automatisiert. Das beginnt mit einem vereinfachten und weniger fehleranfälligen Installationsverfahren der *paedML*-Server mittels Virtualisierung. Außerdem erfolgen Betriebssysteminstallation und Softwareverteilung weitgehend automatisch mit der Open Source Software *Open Server Integration* – kurz: *opsi*. Die Restaurierung wurde ebenso deutlich verbessert, sodass jetzt einzelne oder die gesamten Schüler-Computer in einem Klassenraum innerhalb kürzester Zeit mittels zentraler Steuerung wiederhergestellt werden können.

Mit der *paedML Linux 6.0* haben Sie sich für eine moderne IT-Lösung entschieden, die mit einem professionellen technischen Unterbau ausgestattet ist. Verlässlichkeit und Stabilität kennzeichnen die neue Version, denn Hardwareunterstützung und die Handhabung wurden deutlich verbessert. Technologisch gesehen ist die *paedML Linux 6.0* stärker modular aufgebaut, wodurch die weitere Produktentwicklung in Zukunft flexibler gestaltet werden kann. Wir sind an der Rückmeldung unserer Kunden interessiert und wenn Sie Anregungen oder Wünsche für die Weiterentwicklung der *paedML* haben, bitten wir Sie um Rückmeldung, z. B. über unseren User-Helpdesk.

Die Mitarbeiter der Hotline stehen Ihnen mit Rat und Tat zur Seite, um Sie in der Administration Ihres schulischen Netzwerks zu unterstützen. Die Erfahrung hat gezeigt, dass es ratsam ist lieber einmal zu viel, als einmal zu wenig in der Hotline anzurufen. Wenn Sie Fragen zu Ihrer *paedML Linux* haben, dann kontaktieren Sie bitte Ihre Supportmitarbeiter.

Linux Hotline
0711 – 25 35 83 88
linux-hotline@lmz-bw.de

Geschäftszeiten:
montags – donnerstags 8.00 – 16.00 Uhr
freitags 8.00 – 14.30 Uhr

Dokumentationen zur paedML Linux
Es gibt drei Handbücher für die *paedML Linux*, die sich an verschiedene Zielgruppen richten:

- Das hier vorliegende „**Administrationshandbuch**“ richtet sich an den Netzwerkberater als Systembetreuer der Schule und an den Dienstleister. Hier werden administrative Aufgaben beschrieben, die im Schulalltag getätigt werden können. Darüber hinaus werden hier auch administrative Aufgaben bei der Einrichtung des Schulnetzes beschrieben, die primäre Aufgaben des Dienstleisters sind, der das Schulnetz einrichtet.
- Die „**Installationsanleitung**“, welche die Einrichtung von *VMware*, das Aufsetzen der paedML Infrastruktur und den technischen Aufbau des *paedML*-Netzwerks behandelt, richtet sich ausschließlich an Dienstleister.
- Das „**Handbuch für Lehrkräfte**“, welches die pädagogischen Funktionen Ihrer *paedML Linux* näher beschreibt, erläutert relevante Module für den Unterricht.

Neben diesen drei Handbüchern gibt es weitere Dokumente, die Sie bei der Planung und dem Aufbau eines paedML Linux Netzwerkes unterstützen.

- Der „**Konzeptionsleitfaden**“ bietet eine kurze Einführung in die paedML Linux. Dieses Dokument enthält Hinweise zur Planung der Installation des schulischen Netzwerkes.
- Hinweise für die Ausschreibung des schulischen Netzes und bei der Übergabe des Netzwerks von Ihrem Dienstleister an die Schule finden Sie in unserem „**Ausschreibungsleitfaden**“.
- In einem weiteren Dokument haben wir die „**Hardwareanforderungen**“ der paedML Linux 6.0 zusammengefasst.

Um inhaltliche Doppellungen zu vermeiden, verweisen wir mit Link an gegebener Stelle auf andere Handbücher.

Alle hier genannten Handreichungen zur paedML Linux finden Sie unter http://www.lmz-bw.de/technische-unterstuetzung/kundenportal/linux/dokumentationen.html .

Überprüfen Sie diese Seite bitte regelmäßig nach Aktualisierungen!



Anmerkung zum vorliegenden Administrationshandbuch:
Das vorliegende Werk richtet sich an die Systemrollen „Dienstleister“ und „Netzwerkberater“. Leider sind die Aufgaben der beiden Rollen nicht immer klar voneinander zu trennen, da sowohl der Dienstleister, als auch der Netzwerkberater administrative Aufgaben übernehmen.

In diesem Handbuch finden Sie daher mehr Informationen, als Ihnen als Netzwerkberater recht sein dürfte! Aber vielleicht nicht genug, um den „Geek" (Streber) unter den Netzwerkberatern zufrieden zu stellen?

Als Anbieter der *paedML Linux* stellen wir fest, dass die Bandbreite schulischer Anforderungen in den letzten Jahren immer größer geworden ist. Das hängt zum Beispiel mit den veränderten Lern- und Schulformen und dem Wunsch nach mehr Mobilität und Kollaboration beim Lernen zusammen. Parallel dazu wurden verbesserte Technologien für schulische IT-Lösungen entwickelt, die wir u.a. auch in der paedML integriert haben, um den Wünschen der Schulen gerecht zu werden. Technisch gesehen ist die paedML deutlich innovativer, flexibler und komfortabler geworden. Andererseits hat die Komplexität zugenommen, weil das Spektrum an Möglichkeiten größer geworden ist.

Wir hoffen, dass uns mit unseren Handreichungen der Spagat zwischen diesen unterschiedlichen Anforderungen gelingt.

Wir möchten Sie ausdrücklich darauf hinweisen, dass es nicht Aufgabe des Netzwerkberaters sein sollte, das schulische Netzwerk alleine zu betreuen. Hilfe des Dienstleisters sollte bei Bedarf in Anspruch genommen werden. Wir möchten Sie dennoch dazu ermutigen, bei Bedarf jederzeit in Rücksprache mit unseren Hotline-Kollegen, als Ansprechpartner für die Administration der *paedML Linux* zur Verfügung zu stehen.

Wenn Sie konkrete Anmerkungen zu unseren Dokumentationen haben, dann freuen wir uns auf Ihre Rückmeldung unter

linux-hotline@lmz-bw.de

Typografische Konventionen

Zur besseren Lesbarkeit werden bestimmte Elemente typografisch vom Rest des Textes abgehoben.

- Hervorhebungen in diesem Dokument sind *kursiv*.
- **Besondere Hervorhebungen** sind **fett** ausgezeichnet.
- Ausgaben oder Abfragen von Programmen sind *„kursiv und erhalten Anführungszeichen"*. Ebenso werden Menüs oder Knöpfe, in Programmen und Bedienoberflächen mit Anführungszeichen hervorgehoben.
- Vom Benutzer auszuführende Tastatureingaben an der Linux-Konsole oder an der *Windows* Eingabeaufforderung (zum Beispiel Systembefehle) sowie Auszüge aus Systemdateien, werden durch die `Darstellung in Courier New` vom Rest des Textes abgesetzt. Das Gleiche gilt für Zugangsdaten wie Benutzernamen oder Passwörter.
- Tastenbeschriftungen werden durch Rahmen hervorgehoben.

- Verschachtelte Menüstrukturen werden durch einen senkrechten Strich (|) als Trennzeichen (in der Linux Welt auch „*Pipe*“[1] genannt) voneinander getrennt. So finden Sie zum Beispiel den Zugriff für das Helpdesk-Modul (vgl. Kapitel 18, Seite 252) unter „*Schulkonsole: Unterricht* | *Helpdesk kontaktieren*“.

Unter einigen Kapitelüberschriften finden Sie einen Hinweis, wie Sie den in dem Kapitel beschriebenen Baustein der *paedML Linux* aufrufen können. In der Regel werden konfigurative Änderungen, die in diesem Handbuch beschrieben sind, vom Netzwerkberater ausgeführt. Manche Menüs sind jedoch nur für den Administrator zugänglich. Diese Ausnahmen werden durch Nennung des vom Benutzer „*netzwerkberater*“ abweichenden Benutzernamens gekennzeichnet.

Beispiele:

Aufruf über Schulkonsole (Administrator): Unterricht | Computerraum
Adresse: https://server.paedml-linux.lokal/nagios



Der Aufruf aller internen Webseiten der *paedML Linux* muss über den FQDN (voll qualifizierten Domain-Namen) der jeweiligen Seite geschehen.

Es genügt also nicht bspw. https://server/horde einzugeben, um die Startseite des Webmailers aufzurufen.

Nutzen Sie stattdessen https://server.paedml-linux.lokal/horde .

Hinweise und Tipps werden durch besondere Symbole grafisch vom Text abgehoben:



Durch Hinweis-Felder werden Sie auf Sachverhalte hingewiesen, die Sie beachten sollten, um bestimmte Probleme zu vermeiden, die den Betrieb der *paedML Linux* beeinträchtigen könnten.



Das Tipp-Feld gibt Hinweise, die nicht zwingend notwendig, aber hilfreich sind.



Dieses Feld kennzeichnet Inhalte, die nicht von der Hotline unterstützt werden.

Es handelt sich um Funktionen und Programme, die nicht Bestandteil der Entwicklung der paedML Linux sind. Diese Programme sind in der Regel zu komplex und zu umfangreich, um in Ihrer Tiefe durch die Hotline unterstützt werden zu können.

---

[1] http://de.wikipedia.org/wiki/Pipe_%28Informatik%29

Andererseits bewirken Änderungen in den beschriebenen Funktionen, Abweichungen von Standardeinstellungen der paedML Linux[2].

Aufgrund der besseren Lesbarkeit wird in diesem Handbuch die männliche Form verwendet. Die weibliche Form ist selbstverständlich immer mit eingeschlossen.

[2] In der Entwicklung unserer Produkte setzen wir Standards, die durch die Hotline unterstützt werden (können). Wir bitten Sie um Verständnis, dass es unseren Mitarbeitern nicht möglich ist, auf alle Bedürfnisse en Detail einzugehen. Wir können Ihnen bei manchen Anfragen lediglich Hinweise geben, wie Sie Änderungen am System vornehmen oder wo Sie weitere Dokumentationen zu dem Thema finden können.

1. Übersicht über die paedML Linux

Die *paedML Linux 6.0* bietet viele Neuerungen im Vergleich zu Ihren Vorgängerversionen. Wir wollen Ihnen hier zunächst einen Überblick über die Infrastruktur Ihres Netzwerkes geben (Kapitel 1.1), dann werfen wir einen kurzen Blick auf Benutzerrollen, die in der paedML Linux zum Einsatz kommen (Kapitel 1.2, Seite 20). Das darauf folgende Unterkapitel (Kapitel 1.3 , Seite 21) beschreibt die Werkzeuge, die Ihnen für die Konfiguration der *paedML Linux* zur Verfügung stehen. Im Anschluss an dieses Kapitel erhalten Sie eine Übersicht über nützliche Werkzeuge, die den Systemadministrator bei der Arbeit unterstützen (Kapitel 1.4, Seite 31), sowie ein paar allgemeine Tipps (Kapitel 1.5, Seite 38).

1.1 Geräte und deren Aufgaben

In der folgenden Grafik (große Darstellung in Anhang auf Seite 305) sehen Sie ein *paedML Linux* Netzwerk. Beachten Sie im Zusammenhang mit der Adressierung der Geräte bitte auch die Tabelle auf Seite 66. In diesem Unterkapitel werden wir uns einen Überblick über die Rechner verschaffen, die im Netzwerk der *paedML Linux* zum Einsatz kommen.

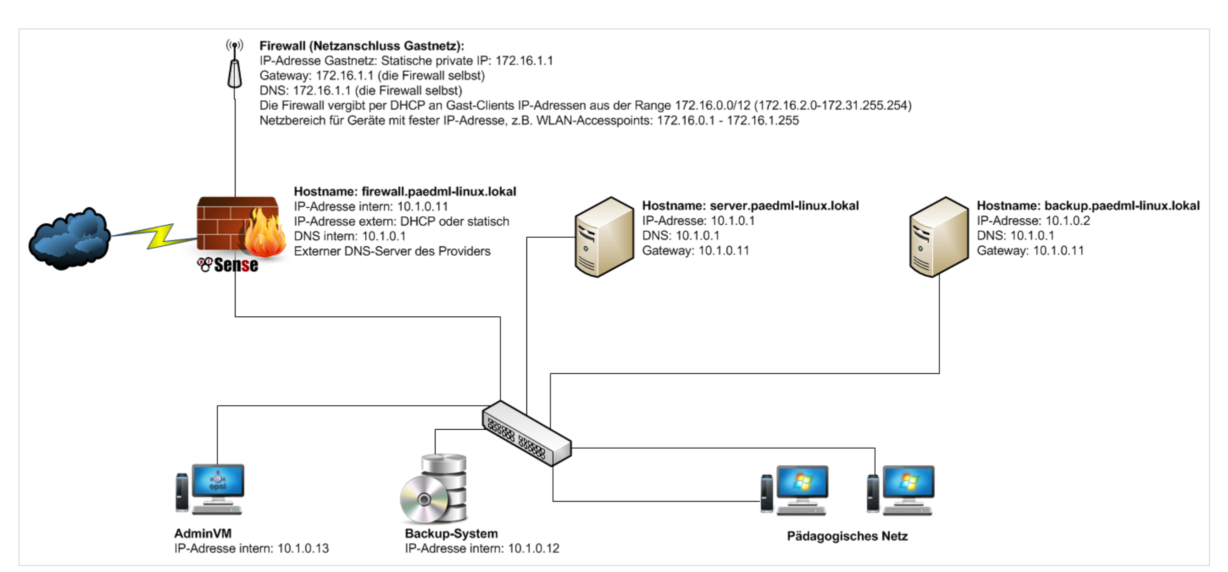


Abb. 1: Übersicht über die paedML Linux

1.1.1 Virtualisierung

Die Server der *paedML Linux* werden virtualisiert ausgeliefert. Während die paedML Linux in früheren Versionen zwar virtualisiert installiert werden konnte, in der Regel aber auf physikalischer Hardware lief, gibt es mit Einführung der paedML Linux 6.0 nur noch die Möglichkeit in einer virtuellen Umgebung zu installieren. Virtualisierung hat den großen Vorteil der Hardware-Unabhängigkeit. Sie benötigen also keine Treiber für Hardwarekomponenten, wenn Sie in einer virtualisierten Umgebung installieren.

Wir empfehlen für die Virtualisierung ausdrücklich einen aktuellen *VMware ESX(i)* Hypervisor[3]. Auf solchen Systemen wird die *paedML Linux* auch in Zukunft weiter entwickelt und getestet. Die paedML läuft zwar auch auf einem anderen Hypervisor, die Hotline leistet allerdings nur für Systeme Support, die mit *VMware* installiert werden.

Die nächste Abbildung zeigt eine schematische Darstellung des Netzwerks der *paedML Linux*. Der Übersichtlichkeit wegen wurde auf Netzwerkkomponenten wie Switches,… verzichtet.

Das Management-Netzwerk muss auf jeden Fall integriert werden, um den *ESXI-Host* zu verwalten. Wir empfehlen einen dedizierten Steuerrechner, die sogenannte „*AdminVM*" als eigenständigen Hardware-Rechner zu betreiben. Dieses Gerät kann für administrative Aufgaben im Schulnetzwerk und ggf. von der Hotline oder Ihrem Dienstleister für Wartungsarbeiten von außerhalb herangezogen werden. Eine Umsetzung der Netzwerkverwaltung über ein dediziertes Management-Netzwerk, mit eigener Netzwerkkarte am Server, ist optional.

In der Virtualisierungsschicht (grün) befinden sich die *paedML Server*, deren virtuelle Netzwerkkarten über virtuelle Switches („*v-Switches*") auf physikalische Netzwerkkarten auf der Hardwareebene (grau) des Virtualisierungsservers verweisen. Zwischen der Hardwareebene und den virtuellen Maschinen liegt der Hypervisor (blau), der auch „Virtualisierungsschicht" genannt wird.

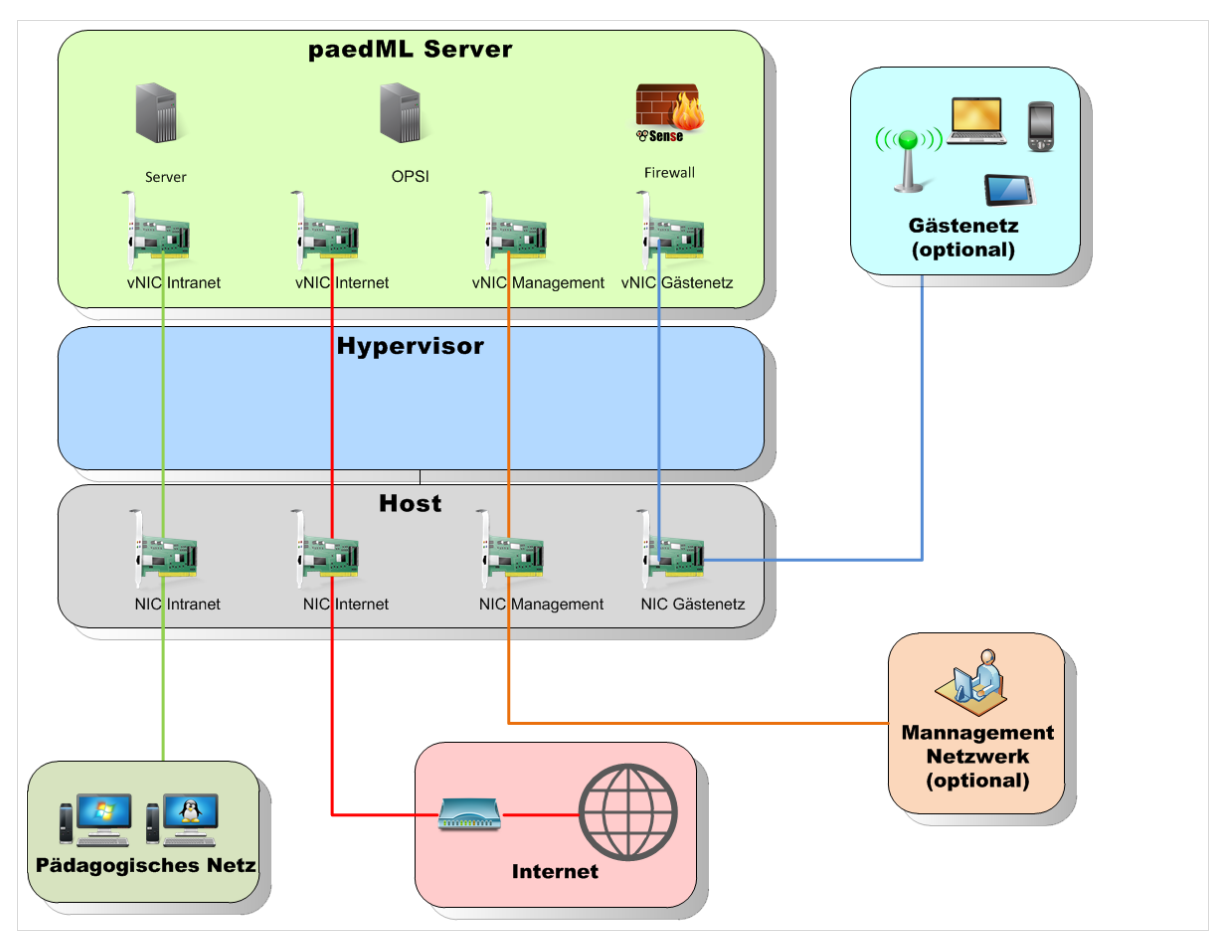


Abb. 2: Schematische Darstellung der Virtualisierung.

[3] Bitte entnehmen Sie die Version den Releasenotes der jeweiligen *paedML Linux* Version.

1.1.2 Firewall pfSense

DNS-Name: firewall.paedml-linux.lokal – IP-Adresse:10.1.0.11
Die Firewall steht als Gateway zwischen dem internen pädagogischen Netzwerk und dem Internet. Sie schützt vor Angriffen von außen und regelt, welche Dienste aus dem schulischen Netzwerk Verbindungen nach außen aufbauen dürfen. Auf dem System ist die auf *FreeBSD* basierende Distribution *pfSense* installiert. Nach der initialen Einrichtung während der Installation des Schulnetzwerkes muss diese Maschine in der Regel nicht weiter konfiguriert werden.

Auf der Firewall läuft ein Zeitserver, über den die Server im Schulnetz mit der aktuellen Uhrzeit versorgt werden. Die Rechner im Schulnetz synchronisieren wiederum Ihre Zeit mit den *paedML*-Servern.

Sie haben die Möglichkeit über ein zusätzliches Netzwerk an der Firewall ein WLAN für schulfremde Geräte in Ihrer Schule einzurichten. Dieses WLAN wird als Gäste-Netz bezeichnet.

Die Firewall wird durch Ihren Dienstleister eingerichtet. Ein Zugriff auf die Konfigurationsoberfläche sollte nicht notwendig werden.

Einige Anpassungen sind im Anhang dieses Dokumentes beschrieben. Wenn Sie weiter gehende Änderungswünsche bezüglich der Firewall-Konfiguration haben, wenden Sie sich bitte an die Hotline.

1.1.3 paedML Server

DNS-Name: server.paedml-linux.lokal – IP-Adresse: 10.1.0.1
Die *paedML* wird mit zwei virtualisierten Servern ausgeliefert. Der eine ist der Master-Server (*Server*), der andere der *opsi Server*. Auf den beiden *paedML* Servern werden verschiedene Dienste, die für den Betrieb der *paedML Linux* notwendig sind, ausgeführt. Hierfür werden manche Dienste auf einer Maschine zur Verfügung gestellt, andere Dienste werden von beiden Systemen ausgeführt.

Die *paedML* Server sind DNS-Server für das interne Netzwerk. Sie brauchen sich beim Betrieb der *paedML* keine IP-Adressen von Maschinen zu merken. Via Namensauflösung sind alle Geräte im schulischen Netzwerk erreichbar.

Auf dem Server laufen – neben den Standard-Linux Systemdiensten – weitere Dienste wie z.B.:

- *Samba 4* – als Domänencontroller mit Active Directory Funktionen
- *Nagios* – ein Werkzeug zur Überwachung verschiedener Parameter Ihrer Hardware und Ihres Netzwerkes
- *Horde* – die Groupware in der *paedML Linux*
- *BackupPC* – die Backuplösung in der *paedML Linux.*

Sie können auf diese Funktionen über die Startseite des Servers (siehe auch Kapitel 1.3.1, Seite21) zugreifen.



Die *paedML Linux* wird mit zwei virtualisierten Servern ausgeliefert. Wir bitten Sie darum, diese beiden Server **IMMER** gleichzeitig zu betreiben, damit die im Hintergrund laufenden Dienste gewährleistet sind.

1.1.4 paedML opsi-Server[4]

DNS-Name: backup.paedml-linux.lokal – IP-Adresse: 10.1.0.2
Auf dem *opsi*- oder *Backup-Server* ist *opsi* (zur Verwaltung von *Windows*rechnern) installiert. Hier laufen die *opsi*-Dienste, durch die die *Windows*-Clients installiert und mit Software versorgt werden. Der Name *Backup-Server* ist historisch aus der Systemrolle im *Univention-Corporate-Server*-Kontext übernommen. In der *paedML Linux* bekommt dieses System als zentrale Aufgabe die Clientverwaltung mit *opsi*. Daher wird das System auch als *opsi-Server* bezeichnet.

Im „*opsi-Depot*" werden Pakete von *Windows*programmen, Installations-Images des Betriebssystems und Systemwerkzeuge abgelegt, die benötigt werden, um einen *Windows*rechner auszuspielen, mit Software zu versorgen und/oder zu warten.

Sie können auf die *opsi*-Konfiguration über die Startseite des Servers (siehe auch Kapitel 1.3.1, Seite 21) zugreifen.



Sowohl Ihr *Server*, als auch Ihr *Backup -Server* können über die in dieser Anleitung beschriebenen Werkzeuge (wie zum Beispiel die *Schulkonsole*) konfiguriert werden. Die Standardkonfiguration des *Backup-Servers* sollte nicht durch Sie oder Ihren Dienstleister verändert werden.

1.1.5 Optional: Webserver

DNS-Name: intranet.paedml-linux.lokal – IP-Adresse: 10.1.0.5



Der hier vorgestellte Webserver ist ein Vorschlag, wie Sie ein eigenes System für Webservices aufsetzen[5] können.

Wir raten Ihnen dringend davon ab, eigene Dienste auf den von uns konfigurierten paedML Servern zu installieren. In diesem Fall wäre ein Verlust des Supportanspruchs nicht ausgeschlossen!

Der Webserver und die darauf installierten Dienste sind NICHT Bestandteil des Supports!

Wenn Sie in Ihrem pädagogischen Netz einen Webserver betreiben wollen, um eigene Dienste (zum Beispiel Vertretungsplan, Testumgebung für Internet-AG,…) im Schulnetz bereit zu stellen, können Sie ein eigenes System aufsetzen und in das Schulnetz integrieren.

Wir empfehlen den Einsatz eines *Univention Corporate Servers*, der im Schulnetz unter der Adresse 10.1.0.5 betrieben wird.

---

[4] Aus Gründen, die dem Unterbau auf Univention Corporate Server geschuldet sind, lautet die Bezeichnung an manchen Stellen auch „*backup-Server*".

[5] Vorgefertigte VM-Ware Images finden Sie zum Beispiel bei http://bitnami.com/stacks oder bei http://www.turnkeylinux.org .

1.1.6 AdminVM

DNS-Name: AdminVM.paedml-linux.lokal – IP-Adresse: 10.1.0.13
Es gibt einige Services für den Betrieb der paedML-Linux (z.B. die *Windows*-Aktivierung, die Definition von Gruppenrichtlinien), die auf einer *Windows*-Maschine laufen müssen. Dafür ist die virtuelle Maschine *AdminVM* vorgesehen.

Die *AdminVM* kann auch auf Hardware installiert werden. In diesem Fall sollte auf dem Gerät ein *vSphere Client* für die *VMware*-Administration und das Programm *Teamviewer* für den Hotline-Zugriff installiert werden.

Da aus lizenzrechtlichen Gründen kein vorinstalliertes *Windows*-System ausgeliefert werden darf, enthält die *VMware*-Vorlage „*AdminVM*“ zwar die Grundkonfiguration der virtuellen Maschine, jedoch noch kein Betriebssystem.

1.1.7 Management-PC

Unter dem Begriff „**Management-PC**“ wird ein physischer PC verstanden, auf dem ein *vSphere-Client* installiert ist. Dieser Rechner ist über das Netzwerk mit dem Virtualisierungs-Host verbunden. Bei der Einrichtung des schulischen Netzes kann ein Rechner des Dienstleisters diese Aufgabe übernehmen.

Vorgehen nach der Installation
Wenn die Installation der *paedML Linux* abgeschlossen ist, wird der *Management-PC* nur noch sporadisch benötigt. Über den *vSphere Client* werden virtuelle Maschinen und/oder der Hypervisor gestartet oder heruntergefahren. Konfigurative Änderungen an der Virtualisierung werden ebenfalls über den *vSphere Client* durchgeführt.

Obwohl aus „Kostengründen“ auch ein Client-PC temporär als Management-PC zweckentfremdet werden könnte, empfehlen wir dringend, für Administrationsaufgaben der paedML Linux einen dedizierten Windows-PC als Management-PC zu verwenden.

Der Vorteil beim Einsatz eines dedizierten *Management-PCs* im Netzsegment „*Internet*“(vgl. folgender Abschnitt) ist, dass Dienstleister oder die Hotline immer auf das System zugreifen können. Dies gilt auch, wenn der Virtualisierungs-Server nicht läuft, da der Zugriff direkt nach dem Router erfolgt. **Wenn das Gerät nicht in Benutzung ist, kann es ausgeschaltet werden.**



Bei *Management-PC* und *AdminVM* handelt es sich um völlig verschiedene Maschinen, die nicht verwechselt werden sollten.

Als Betriebssystem für den *Management-PC* wird *Windows 7* (64 Bit) empfohlen.

1.1.8 NAS als Datensicherungs-System

DNS-Name: nas-backup.paedml-linux.lokal – IP-Adresse: 10.1.0.12

Wir empfehlen Ihnen für die Sicherung des Betriebs der *paedML Linux* eine NAS[6] zu beschaffen, auf der Backup-Dateien abgelegt werden können. Das Thema Backup wird in Kapitel 21, ab Seite 273 beschrieben.

Die Einrichtung des Backup-Systems sehen wir als Aufgabe des Dienstleisters.

1.1.9 Clients und Netzwerkgeräte

DNS-Name: Computername – IP-Adresse: wird bei Rechneraufnahme vergeben
Die Geräte der *paedML Linux* bekommen bei der Aufnahme in die *paedML* eine feste Systemrolle zugewiesen, von der abhängt, wie ein Client verwaltet wird (vgl. Kapitel 4.1.1, ab Seite 66).



Als Client-Betriebssysteme werden *Windows* 7 (64-Bit) und *Windows* 8.1 (64-Bit) unterstützt.

1.1.10 Gäste-Netz für schulfremde Geräte

Das Schulnetz wird durch ein zusätzliches Netzwerk, das *Gäste-Netz*, erweitert.

Wir raten Ihnen aus Sicherheitsgründen dringend dazu, schulfremde Geräte NICHT in das Schulnetz aufzunehmen, sondern über das Gäste-Netz an die IT-Infrastruktur anzubinden.

Besonderheiten:

- Eigenes, vom Schulnetz getrenntes Netz. Adressbereich 172.16.0.0/12 (IP-Adressen von 172.16.0.1 – 172.31.255.254)
- IP-Adressierung per DHCP oder feste IP-Vergabe möglich.
- Keine Anmeldung an schulischen Ressourcen, wie Home- oder Tauschverzeichnissen.
- Proxy-Authentifizierung für Internetaufrufe. Anmeldung mit Domänenkonto (Benutzername und Passwort wie im Schulnetz).
- In den Standardeinstellungen ist nur ein Zugang zu den Protokollen http und https, also nur das Surfen im Internet offen.
- Webfilterung wie im pädagogischen Schulnetz.

1.2 Benutzerrollen der paedML Linux

Um die einzelnen Bereiche wie Unterricht, Pflege der Nutzerdaten und Administration voneinander zu trennen, gibt es in der *paedML Linux* verschiedene Benutzerrollen mit unterschiedlichen Berechtigungen. Die verschiedenen Rollen bestimmen auch darüber, welche Module die Anwender in der *Schulkonsole* angezeigt bekommen. Die Benutzerrollen werden in *nicht administrative* und *administrative* Benutzer unterschieden.

---

[6] Vgl. https://de.wikipedia.org/wiki/Network_Attached_Storage

1. **Nicht administrative Benutzerrollen:**
   1.1. Mitglieder der Gruppe *Schüler* erhalten in der Standardeinstellung nur Zugriff auf Ihr eigenes Kennwort, das sie in der *Schulkonsole* ändern können. Sie können sich mit ihren Benutzerkonten nur an *Windows*-Clients anmelden und die für sie freigegebenen Dateifreigaben und Drucker verwenden.
   1.2. *Lehrer* haben gegenüber Schülern zusätzliche Funktionen in der *Schulkonsole*, mit denen Sie z.B. auf *Schulkonsole*nmodule zugreifen, die das Zurücksetzen von Schülerpasswörtern oder das Auswählen von Internetfiltern ermöglichen. Für die Steuerung des Unterrichts sind pädagogische Funktionen ebenso enthalten.

2. **Administrative Benutzerrollen:**
   2.1. Um administrative Aufgaben im Netz auszuführen, wurde der Benutzer *netzwerkberater* als *paedML*-eigener Benutzer eingeführt.
   2.2. Der Benutzer *domadmin* ist **ausschließlich** für die Rechneraufnahme über die *Schulkonsole* oder den Domänenbeitritt bei der Clientaufnahme erstellt worden. **Mit diesem Konto sollten Sie sich nicht im Schulnetz anmelden.**
   2.3. Vollen Zugriff auf die Administrationsfunktionen der *Schulkonsole* erhält der *Administrator*. Er kann neben den *paedML*-Features auch Einstellungen auf der Betriebssystemebene des Servers vornehmen. Dieses Konto sollte **NUR** bei der Einrichtung des Servers oder dann, wenn es die hier beschriebenen Änderungen erfordern, benutzt werden. Das Benutzerprofil *Administrator* sollte nur dann zum Einsatz kommen, wenn Sie genau wissen, was sie ändern. Eine Dokumentation Ihrer Änderungen hilft bei der späteren Fehlersuche durch die Hotline oder den Dienstleister!

   Der Benutzer *Administrator* kann zudem Änderungen an der Firewall vornehmen und ist administrativer Benutzer des Clientmanagements *opsi*.



Systeminterne Informationen oder Störungen werden per E-Mail an das Konto *netzwerkberater* gesendet. Dieses Konto ist mit einer internen Mailadresse angelegt und muss nicht konfiguriert werden.

Bitte rufen Sie dieses Mailkonto regelmäßig ab (vgl. Kapitel 17 „Mailserver“, Seite 242) und überprüfen Sie, ob ggf. Störungen des Servers vorliegen!

1.3 Wichtige Administrationstools

1.3.1 Startseite

Adresse: https://server.paedml-linux.lokal
Sie erreichen den Server der *paedML Linux* über die folgende URL: https://server.paedml-linux.lokal



Wir empfehlen Ihnen ausdrücklich, administrative Aufgaben über diese Adresse auszuführen. Dort finden Sie eine Übersicht mit allen wichtigen Links zur *paedML Linux*, z.B. über die in der *paedML* verfügbaren Dienste und über externe Angebote, wie z.B. www.lmz-bw.de.

Wie bereits oben beschrieben, müssen Sie in der Regel **nichts** am *Backup-Server* ändern. Im Folgenden werden daher nur die Administratorentools des Servers beschrieben.

Die Startseite des Servers teilt sich in zwei Reiter auf. Der erste Reiter „*Installierte Web-Dienste*“ richtet sich an alle Benutzer. Er enthält drei Links:

1. *„Schulkonsole“* – Über diesen Link gelangen Sie zur *Schulkonsole* (s. Kapitel 1.3.2, Seite 22). Der Inhalt der *Schulkonsole* richtet sich nach der Benutzerrolle (vgl. Kapitel 1.2). Dieser Link führt jeden autorisierten Benutzer (Administratoren und Lehrer) in das Computerraummodul, aus dem die Unterrichtsfunktionen genutzt werden können. Schüler werden zur Passwortverwaltung (Änderung des eigenen Kennwortes) weitergeleitet.
2. *„Horde Groupware“* – Dieser Link führt Sie zu *Horde* (vgl. Kapitel 17, Seite 242).
3. *„Wurzelzertifikat“* – Hier kann das Zertifikat für eine verschlüsselte Kommunikation mit dem Server heruntergeladen werden. Das Zertifikat dient beispielsweise für die Einrichtung von *OpenVPN*-Verbindungen (s. Kapitel 19, ab Seite 255).

Der zweite Reiter *„Administration“* dient als zentraler Anlaufpunkt für die Systemkonfiguration. Hier finden Sie die folgenden Links:

4. *„BackupPC Management“* – Hiermit gelangen Sie zu dem Programm, mit dem Ihr System gesichert werden kann (vgl. Kapitel 21, Seite 273).
5. *„System- und Domäneneinstellungen“* – Über diesen Link gelangen Sie zur *Schulkonsole* (s. Kapitel 1.3.2, Seite 22). Der Inhalt der *Schulkonsole* richtet sich nach der Benutzerrolle (vgl. Kapitel 1.2).
6. *„opsi Windows-Client Management“* – Hinter diesem Link verbirgt sich die Konfigurationsoberfläche für das *opsi*-Clientmanagement, das auf dem *Backup-Server* läuft (vgl. Kapitel 7 ab Seite 116).
7. *„Lokales Nagios“* – Die Übersichtsseite der Monitoring-Software *Nagios* (vgl. Kapitel 16 ab Seite 235) kann über diesen Link erreicht werden.
8. *„opsi-Server“* – Dieser Link bringt Sie auf die Startseite des *Backup-Servers*. An diesem System muss in der Regel nichts konfiguriert werden.
9. *„pfSense Firewall“* – Wenn Sie diesem Link folgen, dann gelangen Sie auf die Konfigurationsmaske Ihrer Firewall.
10. *„Wurzelzertifikat“* – Hier kann das Zertifikat für eine verschlüsselte Kommunikation mit dem Server heruntergeladen werden. Das Zertifikat dient beispielsweise für die Einrichtung von *OpenVPN*-Verbindungen (s. Kapitel 19 „Zugriff von außen “ auf Seite 255)
11. *„Zertifikat-Sperrliste“* – Alte Serverzertifikate können hier eingesehen werden.

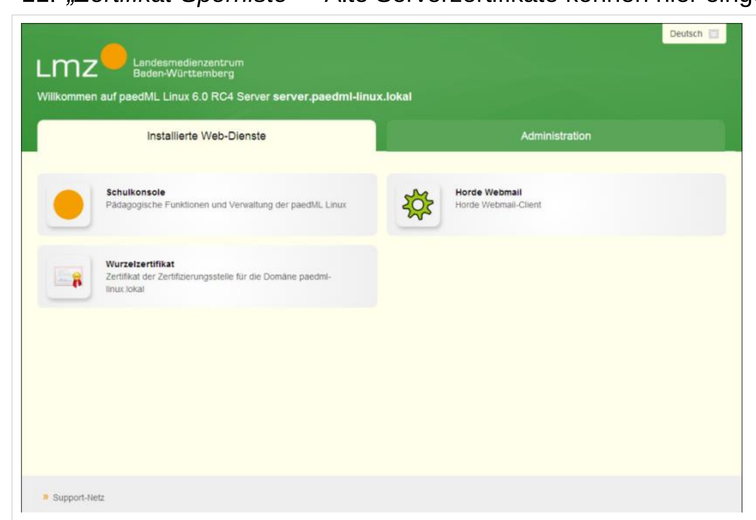


Abb. 3: Die Startseite der Schulkonsole – Anlaufstelle für die meisten steuernden Aufgaben der paedML.

1.3.2 Schulkonsole

Aufruf über Startseite: https://server.paedml-linux.lokal | Knopf „Schulkonsole“

1.3.2.1 Der Aufbau der Schulkonsole

Der Aufbau der *Schulkonsole* ist für alle Benutzer gleich. Er ist in zwei Hauptbereiche unterteilt:

1. Oben finden Sie den Namen des aktiven Servers (*server.paedml-linux.lokal*), und den Namen des jeweils angemeldeten Benutzers. Hier sind vier Symbole, über denen ein Name eingeblendet wird, wenn Sie einen kurzen Moment über dem Symbol verweilen:
   1.1. Mit dem ersten Symbol („*Einstellungen*“) können Sie Lizenzinformationen einsehen, eine neue Lizenz einspielen (Funktion wird von der *paedML Linux* nicht genutzt) und Hilfetexte ein- bzw. ausblenden.
   1.2. Das zweite Symbol („*Hilfe*“) gibt Ihnen weiterführende Hinweise und Hilfefunktionen.
   1.3. Das dritte Symbol blendet „*Benachrichtigungen*“ ein (zum Beispiel, wenn neue Clients aufgenommen wurden).
   1.4. Das vierte Symbol meldet den aktuellen Benutzer von der *Schulkonsole* ab.
2. Das Hauptfenster der Schulkonsole ist in drei Bereiche gegliedert:
   2.1. Oben sehen Sie in Reitern sortiert die Untermenüpunkte. Über dem Reiter „*Übersicht*“, der immer ganz links vorhanden ist, gelangen Sie in das Hauptmenü. Wenn viele Reiter geöffnet sind, können Sie mittels Pfeilen (rechts und links in der Reiterleiste) oder mittels Dropdownmenü (rechts) auf nicht angezeigte Reiter wechseln.
   2.2. Die Hauptmenüs finden Sie im Reiter „*Übersicht“* auf der linken Seite. Wenn Sie Hauptmenüpunkte anklicken, werden die Unterpunkte angezeigt.
   2.3. Im Hauptfenster der Schulkonsole werden die zur Auswahl stehenden Menüpunkte (Reiter „*Übersicht*“) oder der Inhalt des jeweils aktiven Untermenüs angezeigt.

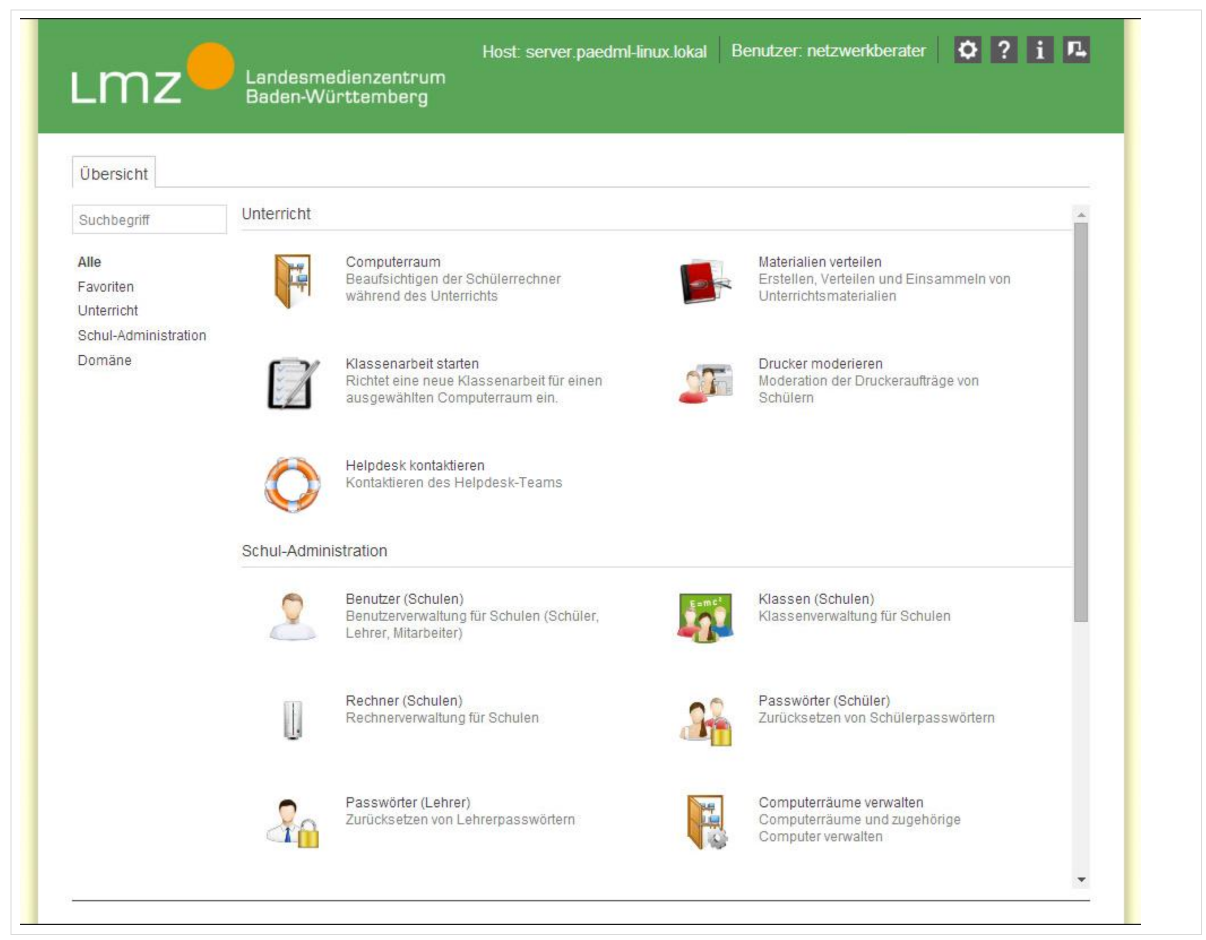


Abb. 4: Schulkonsolenansicht für den Netzwerkberater.

1.3.2.2 Untermenüs

Untermenüs gliedern sich in drei Bereiche:

1. Oben werden die Menüreiter angezeigt. Durch eine Überschrift und (optional) einen kleinen Hilfetext sehen Sie, welchen Bereich Sie konfigurieren und welche Eingaben hierfür notwendig sind. Über ein „*X*“ im Reiter des Menüs kann das Menü geschlossen werden.
2. In der Mitte geben Sie die jeweiligen Informationen ein, die benötigt werden, um ein Objekt anzulegen oder zu modifizieren. Ein Stern (*) kennzeichnet Felder, die eine Eingabe benötigen. Felder ohne Stern sind optional.
3. Der untere Bereich dient der Navigation im Untermenü. Hier können Sie Eingaben abbrechen, auf die vorherige Maske wechseln oder Werte übernehmen.

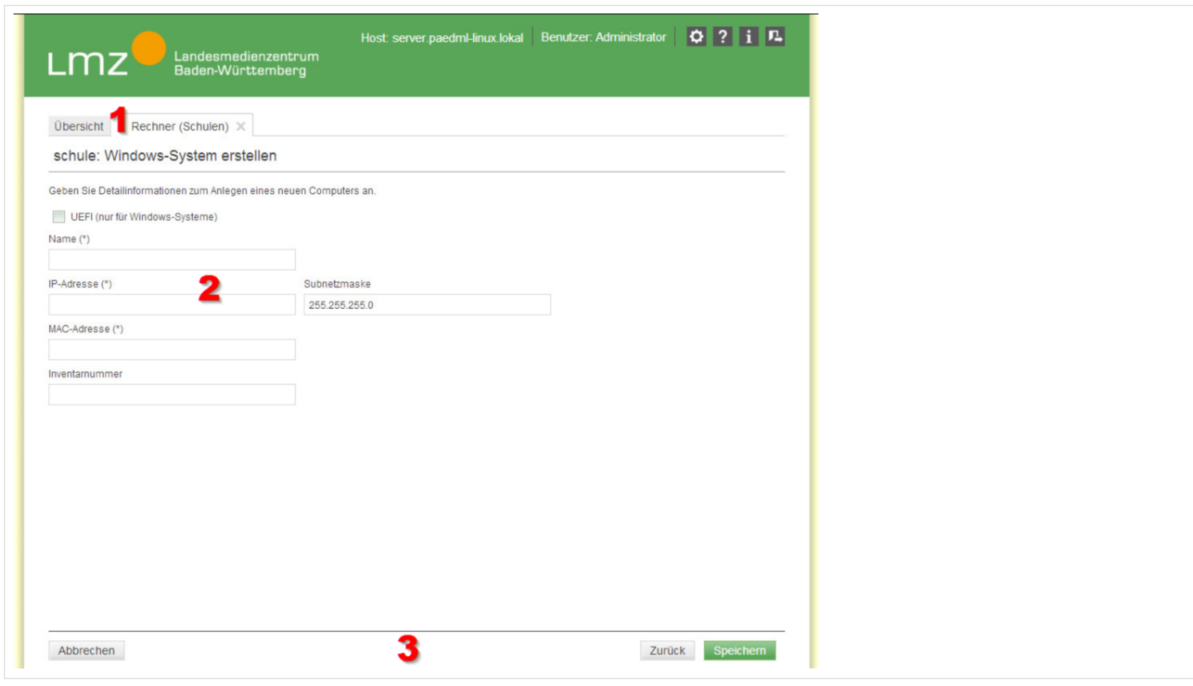


Abb. 5: Ein Untermenü um Computer hinzuzufügen.

1.3.2.3 Schulkonsolenmodule

Die *Schulkonsole* lädt dynamisch Module – abhängig von der Benutzergruppe, der ein Anwender angehört:

1. *Administrative Benutzer* – Administratoren können in der *Schulkonsole* fast alle Anpassungen des Schulnetzwerkes vornehmen. Hier werden zum Beispiel neue Räume, Drucker, Rechner angelegt oder Benutzer verwaltet. Die *Schulkonsole* ist aber auch ein effektives Instrument zur Konfiguration Ihrer Server. **Diese Funktionen sollten nicht (oder nur nach Rücksprache mit der Hotline) genutzt werden!**

   Wie empfehlen Ihnen ausdrücklich, administrative Aufgaben mit dem Benutzer „netzwerkberater“ durchzuführen.
2. *Lehrer* können über die *Schulkonsole* Ihren Unterricht steuern und Ihr Kennwort ändern.
3. *Schüler* können über die *Schulkonsole* lediglich Ihr Kennwort ändern.

Nach Anmeldung an der *Schulkonsole* sehen Sie die für den jeweiligen Benutzer verfügbaren Menüs.



Die folgende Übersicht beschreibt kurz alle im System verfügbaren Menüs und deren einzelne Module.

Sofern wir in unseren Anleitungen nicht explizit auf ein Modul verweisen, bitten wir Sie dringend, keine eigenständigen Veränderungen an einem solchen Modul vorzunehmen.

Die Anforderungen an Schulnetzwerke sind vielfältig. Sie sollten die Möglichkeit haben, Ihr System an die schulischen Bedürfnisse anzupassen. Wir raten Ihnen jedoch dringend davon ab, im Live-System zu experimentieren, um Probleme zu beheben.

Nehmen Sie nur in äußersten Ausnahmefällen Änderungen an nicht dokumentierten Modulen vor, wenn Sie wirklich wissen, was Sie machen!
Dokumentieren Sie alle Änderungen sorgfältig!

Nehmen Sie im Zweifelsfall immer Kontakt mit der Hotline auf!

Melden Sie im Fehlerfall die Änderungen am System an die Hotline, damit die Fehlersuche einfacher wird!



Umsteiger der *paedML Linux* 5.x werden sich vermutlich aus Gewohnheit mit dem Profil *Administrator* (bitte beachten Sie unbedingt den Großbuchstaben im Benutzernamen) an der Schulkonsole anmelden. Wir raten hiervon jedoch ausdrücklich ab!

Die Einstellungsmöglichkeiten des Benutzers *Administrator* reichen tief in das System hinein. Ein unbedachter Klick kann unter Umständen ungewollte Auswirkungen haben. Für die Aufgaben als Netzwerkberater sollte die Anmeldung mit dem Benutzerprofil *netzwerkberater* ausreichend sein.

4. Der Menüpunkt „*Alle*“ beinhaltet – wie der Name schon sagt – alle Menüpunkte.
5. Im Menü „*Favoriten*“ können Sie häufig genutzte Menüpunkte ablegen, um schnell darauf zugreifen zu können. Dieses Menü ist dynamisch und kann von jedem Benutzer individuell gestaltet werden (vgl. Kapitel 1.3.2.4, Seite 28).
6. Der Menüpunkt „*Unterricht*“ beinhaltet die pädagogischen Funktionen der *paedML Linux. Eine Beschreibung der einzelnen Module finden Sie im Lehrerhandbuch.*

Unterricht	
Computerraum	Zugriff auf Schülerrechner via iTalc, Internet-Einstellungen, Rechner sperren, …
Materialien verteilen	Unterrichtsmaterial verteilen und einsammeln
Klassenarbeit starten	Klassearbeit einrichten und starten
Drucker moderieren	Moderation von Druckaufträgen
Helpdesk kontaktieren	Kontakt zu Netzwerkberater im Fall von Problemen bei der IT-Infrastruktur.

Tabelle 1 - Schulkonsolenmodul „Unterricht“.

7. Der Menüpunkt „*Schuladministration*“ deckt die organisatorischen Aufgaben des Netzbetriebes ab.

Schul-Administration	
Benutzer (Schulen)	Benutzer verwalten und anlegen
Klassen (Schulen)	Klassen verwalten und anlegen
Rechner (Schulen)	Geräte verwalten und anlegen
Passwörter (Schüler)	Schülerpasswörter ändern
Passwörter (Lehrer)	Lehrerpasswörter ändern
Computerräume verwalten	Computerräume anlegen und Rechner zuweisen
Lehrer Klassen zuordnen	Lehrer den Klassen zuordnen

Arbeitsgruppen verwalten	Arbeitsgruppen anlegen und verwalten
Internetregeln zuweisen	Internetregeln für Klassen oder Arbeitsgruppen zuweisen
Internetregeln definieren	Internetregeln bearbeiten
Unterrichtszeiten	Unterrichtszeiten definieren
CSV-Import	Benutzerlistenimport
UCS@School Konfigurations-Assistent	Assistent für die Ersteinrichtung des Systems (ohne Funktion, da bereits ausgeführt)

Tabelle 2 – Schulkonsolenmodul „Schuladministration“.

8. Das Schulkonsolenmodul „*Domäne*“ beinhaltet verschiedene Menüs, um die Domänenattribute der Schuldomäne *paedml-linux.lokal* zu konfigurieren.

Domäne	
Benutzer	Verwaltung **aller** Domänennutzer, also auch der Admins und der System-Accounts.
Gruppen	Verwaltung von Benutzer- und Rechnergruppen der Domäne
Rechner	Verwaltung von Rechnern der Domäne
Netzwerke	Konfiguration von Netzwerkeinstellungen
DNS	DNS-Einstellungen der Domäne
DHCP	DHCP-Einstellungen der Domäne
Freigaben	Verwaltung von Verzeichnisfreigaben
Drucker	Verwaltung von Druckern
E-Mail	Verwaltung von Mail-Domänen und Mailinglisten
Nagios	Nagios-Konfiguration
Richtlinien	Verwaltung von domänenweiten Richtlinien
LDAP-Verzeichnis	Durchsuchen und Verwalten des LDAP-Verzeichnisses
Passwort ändern	Änderung des Passworts (des aktiven Benutzers)

Tabelle 3 - Schulkonsolenmodul "Domäne“.

9. Unter „*System*“ finden Sie Menüs, die für den jeweiligen Server (Master-Server oder *Backup-Server*) aktiv sind.

System	
Statistiken	Nutzungsstatistiken zur Auslastung der Maschine (CPU/Swap/Speicher)
App Center	Installation von Apps und Software
Domänenbeitritt	Domänenbeitritt des lokalen Systems
Univention Configuration Registry	Verwaltung von UCR-Variablen des lokalen Systems
Prozessübersicht	Prozessübersicht des lokalen Systems
Dateisystem Quota	Konfiguration von Quota für das lokale System
Neustarten	Herunterfahren oder Neustart des lokalen Systems
Software-Aktualisierung	Überblick über verfügbare Aktualisierungen für lokales

	System
Druckaufträge	Verwaltung von Druckaufträgen der lokalen Drucker
Systemdienste	Übersicht und Konfiguration lokaler Systemdienste
Hardwareinformationen	Übersicht über Hardwareinformationen des lokalen Systems
Basis-Einstellungen	Konfiguration grundlegender Einstellungen des lokalen Systems

Tabelle 4 - Schulkonsolenmodul "System".

10. Das letzte Schulkonsolenmodul „*Installierte Applikationen*“ schließlich gibt eine Übersicht über die verschiedenen Softwarepakete, die für den Betrieb der *paedML Linux* auf dem Server installiert sind. **Hier dürfen Sie keine Änderungen vornehmen!**

1.3.2.4 Favoriten

Jeder Benutzer hat die Möglichkeit, häufig benutzte Menüpunkte als *Favoriten* in einem eigenen Menü abzulegen. Dieses Hauptmenü sehen Sie im Reiter „*Übersicht*“ der Schulkonsole.

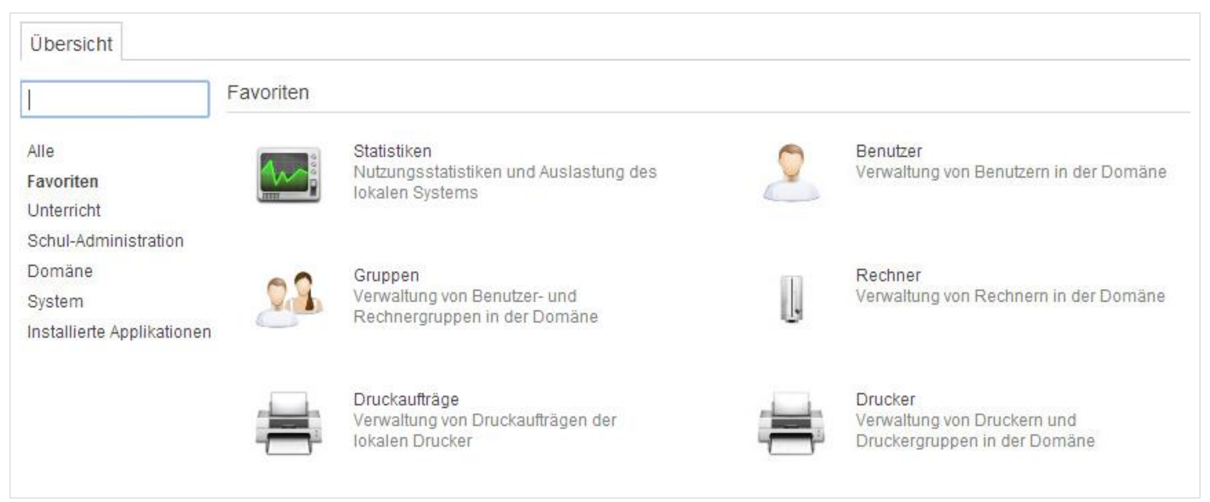


Abb. 6: Favoriten.

Um einen Menüpunkt zu den Favoriten hinzuzufügen, klicken Sie mit der linken Maustaste einmal auf den jeweiligen Menüpunkt. Ein *neues Menüsymbol* erscheint. Wenn Sie dieses Symbol anklicken, öffnet sich ein Dialog, mit dem Sie die Möglichkeit erhalten, den Menüpunkt zu den Favoriten hinzuzufügen oder aktive Favoritensymbole aus den Favoriten zu entfernen.

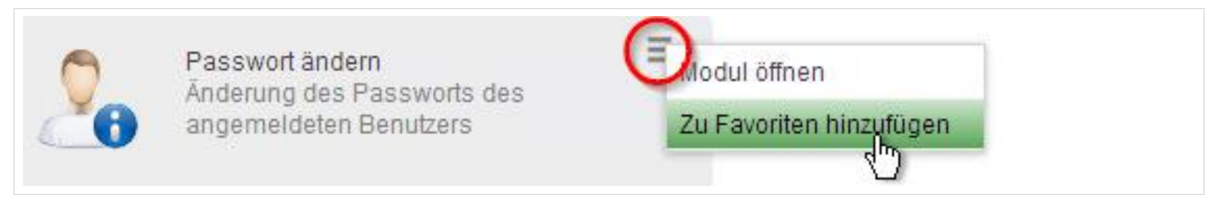


Abb. 7: Favoriten können Sie selbst verwalten.

1.3.3 Univention Configuration Registry

Aufruf über Schulkonsole: System | Univention Configuration Registry
Einige Parameter der *paedML Linux* werden über die „*Univention Configuration Registry*“ (kurz „*UCR*“) konfiguriert.



Falsche Einträge in der *UCR* können zu unerwünschten Effekten führen. Dieses Modul ist mächtig und relativ komplex, weniger in der Bedienung, jedoch im Funktionsumfang und in den Auswirkungen von Änderungen.

Wir möchten Sie ausdrücklich darauf hinweisen, dass Sie Änderungen an der UCR nur dann vornehmen dürfen, wenn Sie sich im Klaren darüber sind, was diese Änderungen im System bewirken.

BESSER IST ES, IN DIESEM MODUL NICHTS ZU ÄNDERN!

Dokumentieren Sie jede Änderung und teilen Sie Änderungen im Fehlerfall der Hotline mit!

In diesem Handbuch werden an ein einigen Stellen Parameter der *UCR* und deren Optionen beschrieben. Das Verfahren zum Ändern dieser Parameter wird nur hier beschrieben.

Sie öffnen das Schulkonsolenmodul „*Univention Configuration Registry*“ in der *Schulkonsole* über dem Menüpunkt „*System* | *Univention Configuration Registry*“.

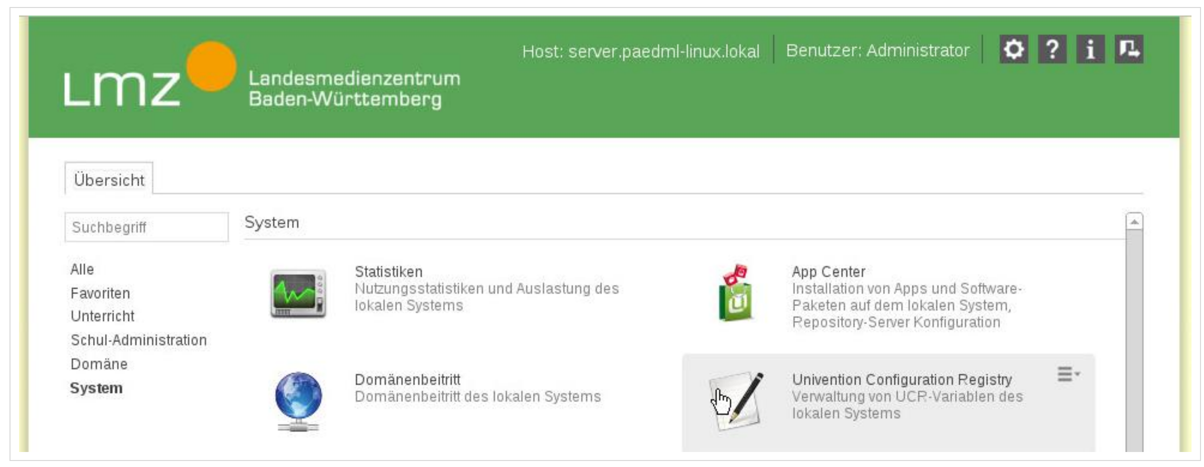


Abb. 8: Aufruf des UCR-Moduls.

Es öffnet sich ein neuer Reiter, in dem ALLE *UCR-Variablen* angezeigt werden. Um eine bestimmte Variable zu finden, können Sie ein „*Schlüsselwort*“ in das gleichnamige Feld eintragen. Die Suche kann über die Angabe einer „*Kategorie*“ oder der Auswahl eines Wertes im Feld „*Suchattribut*“ verfeinert werden. Mit Klick auf „*Suchen*“ startet Ihre Suche.

Die Suchergebnisse werden im Hauptfenster angezeigt. Um eine *UCR-Variable* zu ändern, markieren Sie die Checkbox („Haken“) vor der Variablen. Anschließend werden oberhalb der Variablen (neben

dem „*Hinzufügen*“-Knopf) zwei weitere Knöpfe „*Bearbeiten*“ und „*Löschen*“ angezeigt. Mit Klick auf „*Bearbeiten*“ öffnet sich ein neuer Dialog.



Abb. 9: Auswahl der UCR-Variable „squid/webports“ für die Bearbeitung.

Im Dialogfenster „*UCR-Variable bearbeiten*“ können Sie Änderungen der Variablen vornehmen. Viele Variablen haben im Beschreibungstext eine Erläuterung zu den Parametern. Übernehmen Sie die Änderungen mit „*Speichern*“.



Abb. 10: Änderung einer UCR-Variable.

1.3.4 opsi configed editor

Aufruf über Startseite https://server.paedml-linux.lokal | Reiter „Administration“ | Knopf: „opsi *Windows*-Client Management“ oder Aufruf über lokal installierten opsi-Client.

Der *opsi configed Editor* ist ein Java Programm, mit dem sich *Windows*-Clients grafisch verwalten lassen. Das Programmpaket *opsi*, das für die Softwareverteilung benötigt wird, ist in Kapitel 7 ab Seite 116 beschrieben.

1.3.5 Kommandozeile oder Konsole

Die (Server) -Kommandozeile wird in der *paedML Linux 6* weitaus weniger als in älteren Versionen benötigt. Über die Eingabe von Befehlen können Sie zum Beispiel Programme starten, Dateien editieren oder Inhalte auf dem Server suchen. Die Konsole erscheint auf den ersten Blick kompliziert, stellt aber ein sehr effektives und wirksames Werkzeug dar.

Mit der *paedML Linux* können Sie fast alle Aufgaben über die grafische Benutzeroberfläche durchführen. Diese wurde in der Version 6.0 neu und intuitiv gestaltet. Menüs mit möglichst einfacher Bedienung lösen können. Nur wenige Vorgänge lassen sich nur über Konsolenbefehle abbilden.

Konsolenbefehle werden wir für Sie möglichst genau dokumentieren. Außerdem helfen Ihnen die Mitarbeiter der Hotline gerne im Zweifelsfall mit Rat und Tat zur Seite.

```
root@server:/home/Administrator# ls -alh
insgesamt 28K
drwx--x--x  4 Administrator Domain Admins 4,0K 25. Nov 14:35 .
drwxr-xr-x 10 root          root          4,0K 25. Feb 14:13 ..
-rw-------  1 Administrator Domain Admins 3,2K 25. Nov 14:35 .bashrc
-rw-------  1 Administrator Domain Admins  675 25. Nov 14:35 .profile
-rw-r--r--  1 Administrator Domain Admins 2,3K 10. Feb 13:28 .univention-server-join.log
drwxr-xr-x  2 Administrator Domain Admins 4,0K 25. Nov 14:35 .univention-skel
-rw-------  1 Administrator Domain Admins    0 25. Feb 14:23 .univention-skel.lock
drwx------ 11 Administrator Domain Admins 4,0K 25. Nov 14:35 windows-profiles
root@server:/home/Administrator#
```

Abb. 11: Das Homeverzeichnis des Administrators an der Konsole.

1.4 Nützliche Werkzeuge

Die Liste der Werkzeuge für die Arbeit mit Computern ist groß und die Vorlieben der Benutzer sind verschieden. Häufig erfüllen verschiedene Programme denselben Zweck. Wir möchten Ihnen hier ein paar Programme vorstellen, die Ihnen die Arbeit im schulischen Netzwerk erleichtern.

1.4.1 OpenVPN

Das Programm *OpenVPN* ermöglicht einen Fernzugriff von entfernten Rechnern in das Schulnetz. Mithilfe dieses Programmes kann Unterrichtsmaterial von zu Hause in das eigene Homeverzeichnis übertragen werden. Der Administrator kann theoretisch[7] von zu Hause aus Wartungsarbeiten durchführen. Die Beschreibung zu *OpenVPN* finden Sie in Kapitel 19 „Zugriff von außen “auf Seite 255.

1.4.2 PuTTY – der Alternative Weg zur Serverkonsole

Der ssh-Client *PuTTY* stellt Verbindungen zu (Linux-) Servern her, auf denen der Dienst das Protokoll *ssh*[8] verfügbar macht. Dadurch können Sie von einem *Windows*rechner aus über das Netzwerk auf die Kommandozeile Ihres Servers zugreifen und dort Befehle ausführen. *PuTTY* ist eine Alternative zur

---

[7] In der Praxis empfiehlt es sich für Wartungsaufgaben vor Ort zu sein!

[8] http://de.wikipedia.org/wiki/Secure_Shell

Arbeit an der Serverkonsole. Administrative Aufgaben können von einem *Windows*rechner aus erledigt werden.

Einen Downloadlink finden Sie unter http://www.chiark.greenend.org.uk/~sgtatham/*PuTTY*/download.html .

Beim Aufruf von *PuTTY* erscheint eine Anmeldemaske, in der Sie den Namen oder die IP-Adresse des fernzusteuernden Servers (Feld „*Hostname (or IP-Adress)*“) sowie den „*Port*“ für den Fernzugriff eintragen müssen. Sie können die Werte für einen späteren Zugriff speichern. Geben Sie hierfür in das Feld unter „*Saved Sessions*“ einen Namen ein.

Ein Klick auf „*Open*“ oder ein Doppelklick auf ein gespeichertes Serverprofil öffnet eine Verbindung zum jeweiligen Server.

System	Adresse	Port
Server von intern	server.paedml-linux.lokal	22
Server von außen	IP-Adresse des Schulnetzes / DynDNS-Name	22222 (muss ggf. in der Firewall aktiviert werden)
Backup-Server von intern	backup.paedml-linux.lokal	22
Backup-Server von außen	IP-Adresse des Schulnetzes / DynDNS-Name	22223 (muss ggf. in der Firewall aktiviert werden)

Tabelle 5: Adressen für den Zugriff auf die paedML Server.

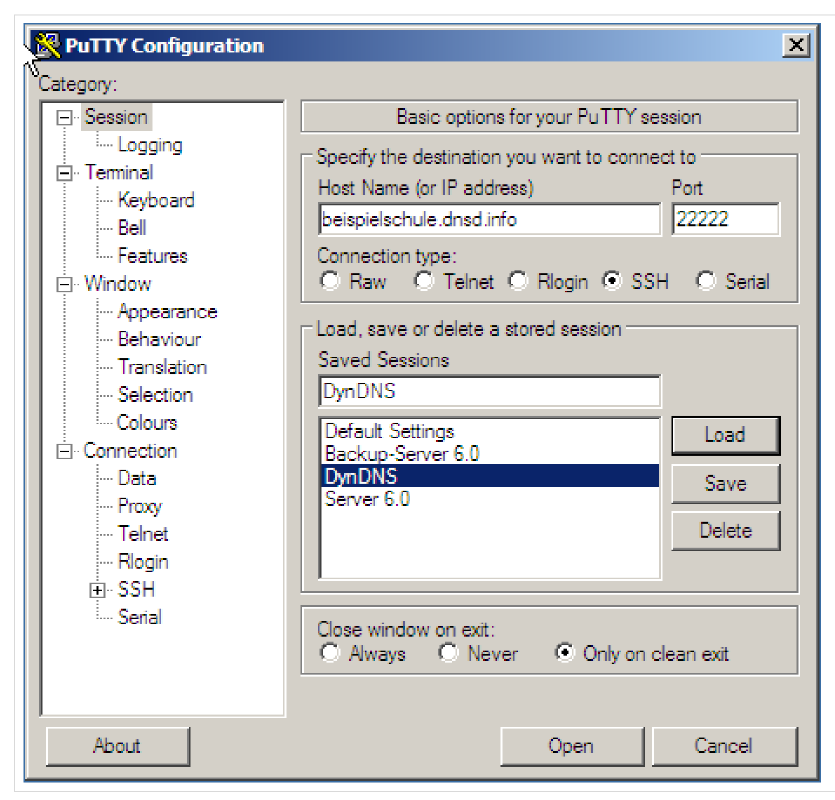


Abb. 12: PuTTY *– Welchen Server hätten Sie gern?*

Die Anmeldung am jeweiligen Zielserver geschieht mit Benutzername und Passwort des Servers. Empfohlener Benutzer ist der *Administrator*.

Nach erfolgreichem Login haben Sie mit *PuTTY* eine vollwertige Serverkonsole, mit der Sie Befehle an den Server senden können. Die Abmeldung erfolgt über den Befehl `exit` oder durch Schließen der *PuTTY*-Konsole.

```
root@server: ~
login as: root
Using keyboard-interactive authentication.
Password:
Univention DC Master 3.2-1:

The UCS management system is available at https://server.paedml-linux.lokal/ (10.1.0.1)

You can log into the Univention Management Console - the principal tool to manage
users, groups, etc. - using the "Administrator" account and the password selected
for the root user on the master domain controller.


Last login: Wed Mar 26 12:54:29 2014 from 1
root@server:~# exit
```

Abb. 13:Eine PuTTY*-Konsole nach erfolgter Anmeldung.*

1.4.3 WinSCP und Explorer – Datenaustausch mit dem Server



WinSCP ermöglicht Ihnen den Zugriff auf die Verzeichnisstruktur des Servers und kann beispielsweise für das Übertragen von *opsi*-Paketen verwendet werden.

Wenn Sie Daten (beispielsweise für den Benutzerimport) nur im Home-Verzeichnis des Administrators ablegen wollen, können Sie auch den *Windows-Explorer* nutzen.

WinSCP
WinSCP ist eines von vielen Programmen, das Ihnen den Datenaustausch zwischen *Windows*-Systemen und dem Linux-Server ermöglicht. Dadurch können Sie zum Beispiel Benutzerlisten auf den Server übertragen. Die Software steht als *opsi*-Paket zur Verfügung und kann einfach auf Clients, die mit *opsi* verwaltet werden, installiert werden.

Sie können *WinSCP* aber auch direkt vom Hersteller herunterladen und installieren (http://winscp.net/eng/docs/lang:de).

Wenn Sie *WinSCP* auf Ihrem Arbeitsplatz installiert haben und die Anwendung aufrufen, öffnet sich ein Anmeldefenster. Hier geben Sie die Zugangsdaten für den Rechner an, mit dem Sie sich verbinden wollen. Sie können auf den Server intern, (also innerhalb des Schulnetzes), oder auch von außerhalb des Schulnetzes zugreifen. Der Zugriff von außen kann beispielsweise durch den Dienstleister geschehen. Hierfür müssen in der Firewall im Menüpunkt „*Firewall* | *NAT*“ und dort im Reiter „*Port*

Forward“ die vordefinierten Zugriffsregeln aktiviert werden (vgl. Anhang „Firewallkonfiguration“ Seite 297). Die Regeln sind im Auslieferungszustand deaktiviert.

Der Zugriff auf das jeweilige System geschieht über den „*Rechnernamen*“ (bzw. die IP-Adresse bei Zugriff von außen), die jeweilige „*Portnummer*“, den „*Benutzernamen*“ und das zugehörige „*Kennwort*“.

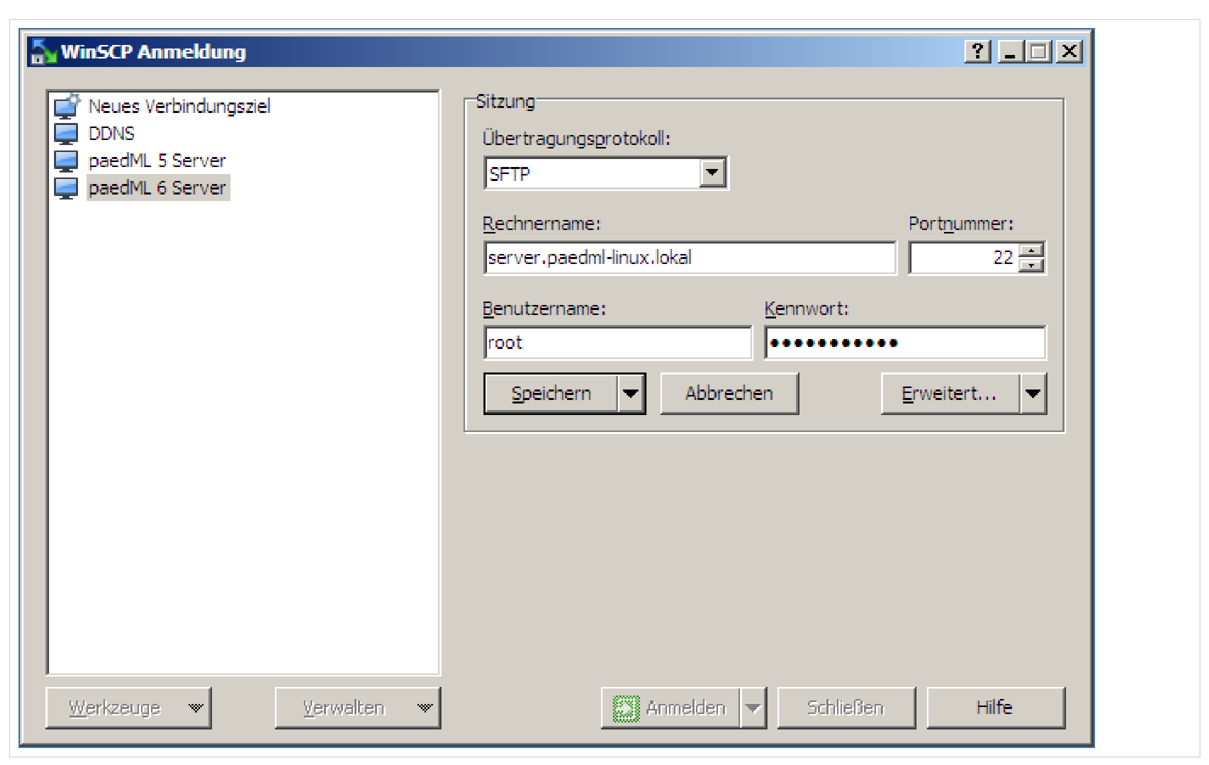


Abb. 14: Anmeldedaten beim Aufruf von WinSCP.

Es öffnet sich ein neues Fenster. Auf der linken Seite ist zunächst der lokale Rechner, auf dem das Programm aufgerufen wurde. Auf der rechten Seite befindet sich der Rechner, auf den Sie zugreifen wollen.

Sie können nun Daten zwischen den beiden Systemen austauschen. Markieren Sie hierfür die entsprechenden Dateien und verschieben Sie diese per „Drag and Drop“ oder nutzen Sie die Schaltflächen im oberen Viertel des Programmes.

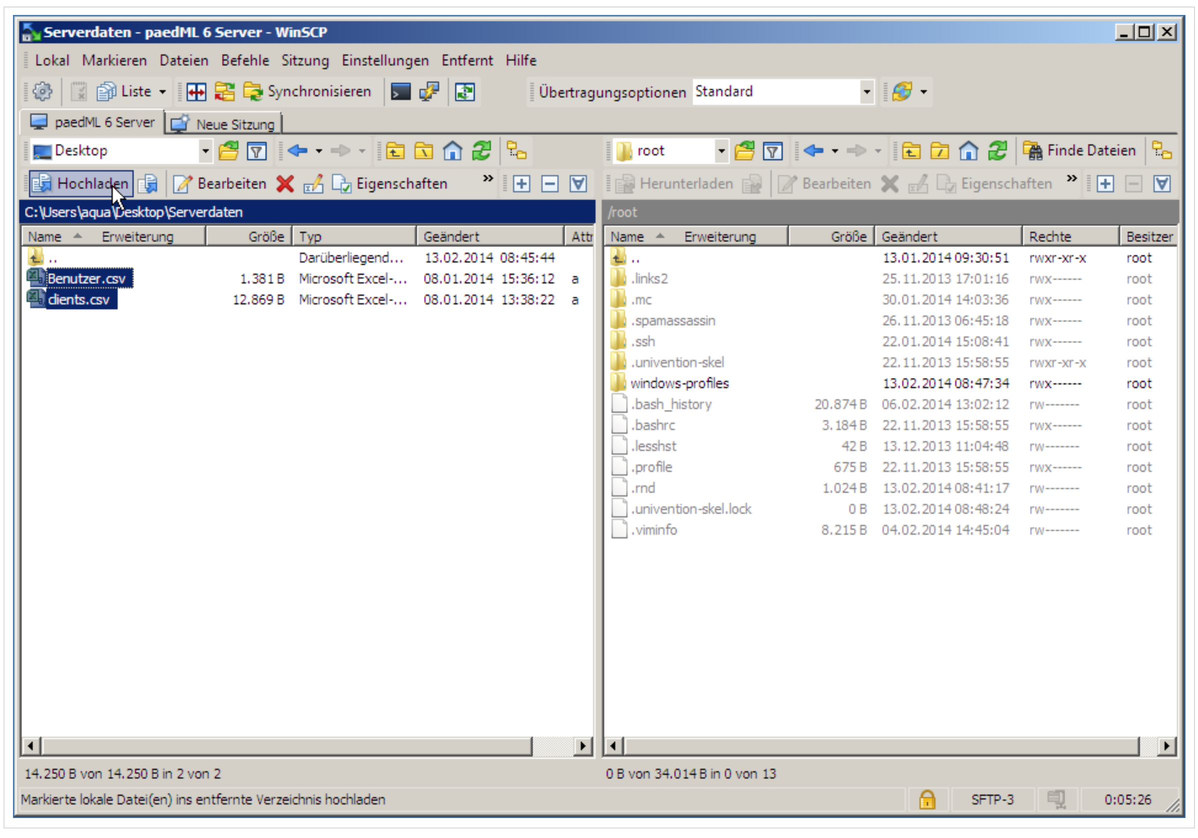


Abb. 15: WinSCP in Aktion.

***Windows*-Explorer**

Während mit *WinSCP* Zugriff auf alle Verzeichnisse der Server möglich ist, ist der Zugriff durch den *Windows-Explorer* begrenzt. Hier können unter *Windows* angemeldete Benutzer nur auf *Windows*-Freigaben zugreifen, die auf Server erreichbar sind. Hinweise zur Verzeichnisstruktur finden Sie in Kapitel 20, ab Seite 264.

Für bestimmte administrative Aufgaben ist ein eingeschränkter Zugriff ausreichend. Als Beispiel sei die Übertragung von Benutzer- und Rechnerlisten für den Import an der Konsole genannt.

Im folgenden Beispiel sehen Sie den Zugriff von *Windows* auf das Homeverzeichnis *H:* des Administrators. Melden Sie sich hierfür als Administrator der Domäne mit „*Administrator@paedml-linux*“ und dem zugehörigen Kennwort an einem *Windows*-Rechner an.

Auf dem Desktop liegt die Verknüpfung „*Computer*“ (1) über die Sie zu einer Übersicht der lokalen Laufwerke des Rechners, sowie der für den jeweiligen Benutzer verfügbaren Netzwerkfreigaben gelangen.

Öffnen Sie nun die Netzwerkfreigabe „*Administrator (\\server) (H:)*“ (2), um in das Homeverzeichnis des Administrators zu gelangen.

Sie können anschließend eine auf dem Desktop abgelegte Benutzerliste in das Verzeichnis übertragen (3).

Abb. 16: Anmeldung im Home-Laufwerk des Administrators.



Alle Domänen-Benutzer (und damit auch der Administrator) können über die Eingabe von „*H:*“ in der Adressleiste des *Windows-Explorers* jederzeit auf das eigene Home-Laufwerk zugreifen.

1.4.4 Editoren

Häufig gehen Anpassungen am System mit Änderungen an (Konfigurations-) Dateien einher. Der beständige Wechsel der Systembenutzer ist ein Beispiel dafür. Neue Schüler, neue Lehrer kommen, alte müssen gelöscht werden. Um Dateien zu ändern, werden Bearbeitungsprogramme, sogenannte Editoren, eingesetzt. Mit diesen Programmen können Sie Dateien öffnen, modifizieren und die neue Datei speichern.

Die Wahl eines Editors ist abhängig vom Geschmack des Anwenders. Es gibt Programme, die direkt auf dem Server ausgeführt werden können (*vi*, *mcedit*, *nano*,…) und Programme, die unter *Windows* laufen. Erstere sind schlank, an der Serverkonsole verfügbar, aber zum Teil wenig intuitiv. Letztere bieten einen

höheren Komfort (Mausbedienung, Plugins,..) und eine einfachere Bedienbarkeit. Aus der Vielfalt der Bearbeitungsprogramme wählen wir zwei aus und sie Ihnen kurz vor. Welchen Editor Sie benutzen, bleibt letztlich Ihnen überlassen.

notepad++

Ein unter *Windows* weit verbreiteter Editor ist das Programm *notepad++.* Wir empfehlen Ihnen die Installation des Editors. Dieser relativ einfach zu bedienende Editor hat den Vorteil, dass er Kodierungen konvertieren kann.



Wir empfehlen Ihnen *notepad++* für das Bearbeiten von Dateien zu verwenden. Dieser Editor wird – bei richtiger Einrichtung – automatisch auf die *AdminVM* installiert und ist dort verfügbar.

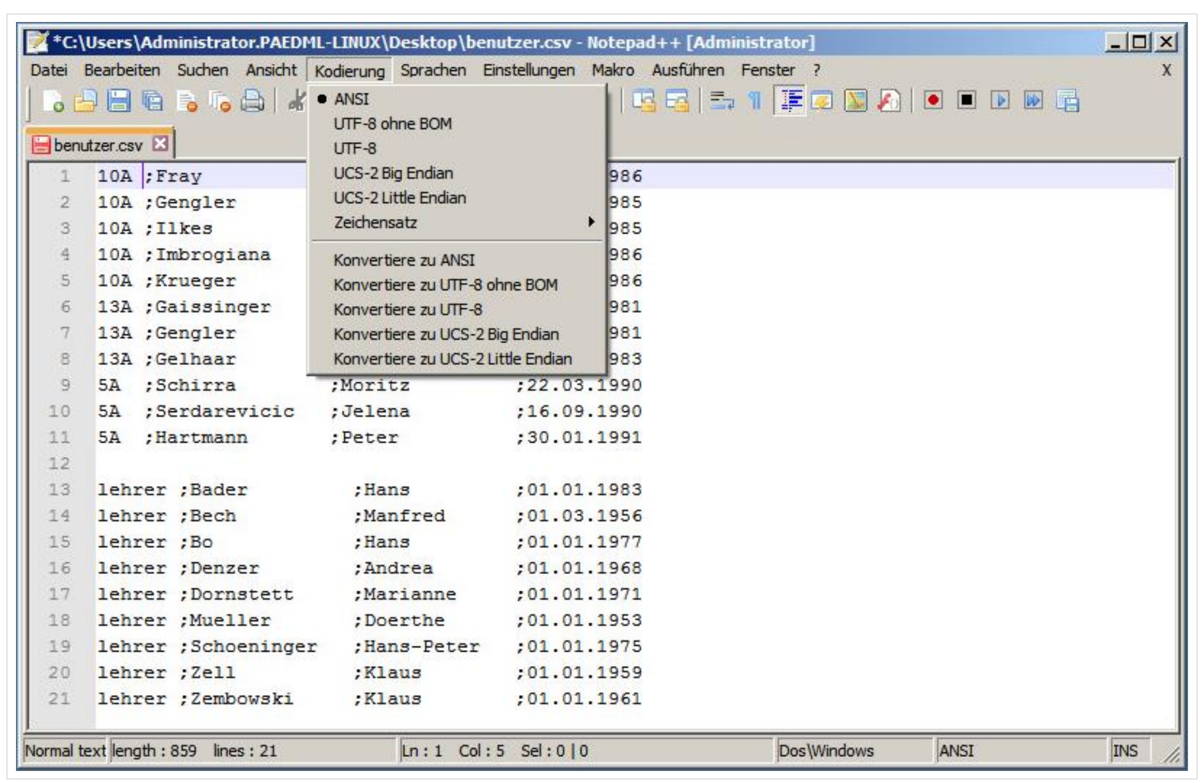


Abb. 17: Eine Benutzerliste im Editor Notepad++

jedit

Im Auslieferungszustand der paedML Linux ist das *opsi*-Paket *jedit* enthalten. *jedit* benötigt ein installiertes *java* auf dem Client von dem aus es ausgeführt wird*. java* wird automatisch für die Installation ausgewählt, wenn *jedit* installiert wird.

Sofern Sie *opsi*-Pakete konfigurieren bietet *jedit* einen entscheidenden Vorteil: Es unterstützt Syntax-High-Lightning, also die Hervorhebung von *opsi*-Syntax.

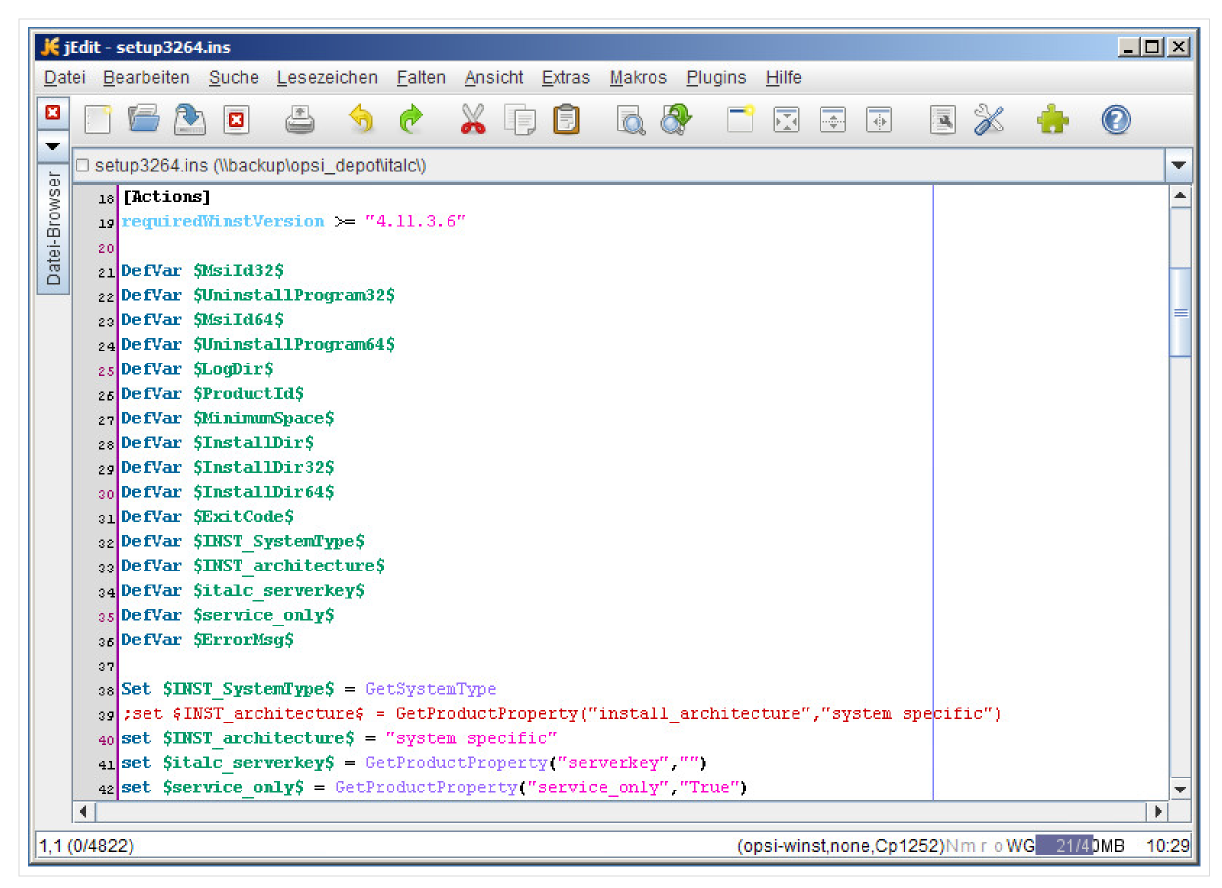


Abb. 18: jedit mit opsi-Syntax-High-Lightning.

1.5 Allgemeine Hinweise

Dieses Unterkapitel soll Ihnen ein paar Tipps und Anregungen für häufig vergessene oder „stiefmütterlich“ behandelte Themen im Kontext des schulischen IT-Umfeldes geben. Die Themen treten immer wieder in Beratungssituationen der Hotline auf und finden hier Ihren Platz. Der Weisheit letzter Schluss kann hier nicht angeboten werden. Es gilt daher abzuwägen, in welchem Verhältnis Mehrwert und Aufwand in Ihrem Schulnetz stehen. So führen wir hier beispielsweise Überlegungen zum Sperren von USB-Sticks aus, die der Philosophie der Datensicherung privater Daten durch die Anwender entgegenstehen. Ein Kompromiss wäre der Einsatz eines Virenscanners, um Schadsoftware aus dem Netzwerk fern zu halten und USB-Sticks für die individuelle Datensicherung der Anwender freizugeben.

1. **Legen Sie immer Sicherungskopien von Dateien an bevor Sie darin Änderungen vornehmen.** Dateien sind schnell verändert, die ursprünglichen Werte gehen aber dauerhaft verloren. Auch wenn eine Datei auf den ersten Blick „richtig“ aussehen sollte, so kann es sein, dass wichtige Details fehlen.

   Ein Beispiel aus der Datei /etc/ldap/slapd.conf:

```
suffix          "dc=paedml-linux,dc=lokal"     (Original)
suffix          dc=paedml-linux,dc=lokal       (Fälschung)
```

Wenn Sie diese Zeilen isoliert betrachten, springt Ihnen als Leser sofort ins Auge, dass in der zweiten Zeile keine Anführungszeichen enthalten sind. Wenn Sie diese Zeile im Kontext einer Konfigurationsdatei betrachten, könnten Sie dieses Detail schnell überlesen.

Wenn Sie von der ursprünglichen Datei ein Backup angelegt haben, dann können Sie mit dem Linuxbefehl `diff` herausfinden, wo Veränderungen vorgenommen wurden:

```
root@server:/etc/ldap# diff slapd.conf slapd.conf.alt
91c91
< suffix "dc=paedml-linux,dc=lokal"
---
> suffix dc=paedml-linux,dc=lokal
```

2. **Erstellen Sie regelmäßig Sicherungen Ihres Systems.** Insbesondere vor „größeren Eingriffen" empfehlen wir Ihnen, eine Komplettsicherung der paedML Server und der Nutzerdaten anzulegen. Sie können auch alternativ die Benutzer für Ihre eigene Datensicherung verantwortlich machen. So entlasten Sie sich ungemein, falls der „Daten-Gau" eintreten und die Daten Ihres Servers gelöscht werden sollten. **Die Mitarbeiter der Hotline werden gegebenenfalls nur in Ihr System eingreifen, wenn Sie uns versichern können, dass Sie ein funktionierendes Backup vorliegen haben.**

3. Eine **Sicherung von Nutzerdaten** führt bei Datenverlust (durch Serverausfall oder ähnlichem) zu einem Mehraufwand beim Zurückspielen der Daten. Eine durchaus erwägenswerte Alternative wäre es, den **Anwender**n klar zu machen, dass sie selbst **für das Sichern Ihrer Daten** verantwortlich sind. Da im Auslieferungszustand Wechseldatenträger gesperrt sind, sollten Sie über eine Freigabe von USB-Sticks nachdenken (s. letzter Punkt dieser Liste und Kapitel 12.4, ab Seite 193)

4. In diesem Kontext sollten Sie auch darüber nachdenken, wie **Homeverzeichnisse regelmäßig aufgeräumt** werden. Speicherplatz ist heute nicht mehr unbedingt ein finanzielles Problem, dennoch sammeln sich – vor allem bei vielen Benutzern – mit der Zeit einige Daten an. Bevor es hierbei zu Kapazitätsproblemen kommt, sollten nicht benötigte Daten gelöscht werden. Der Schuljahreswechsel bietet sich für ein „Großreinemachen" an.

5. Ein wichtiger Bestandteil für den Umgang mit PCs in der Schule ist eine **Nutzungsordnung**[9], **die alle Schüler – beziehungsweise deren Erziehungsberechtigte – unterschreiben** müssen. Hier wird der Umgang mit dem Schulnetz geregelt und die Grundlage für die Ahndung von Verstößen gelegt. Die paedML Linux bietet mit Funktionen wie der Druckermoderation oder der Möglichkeit für Lehrer, den Bildschirminhalt von Schülern einzusehen, den Zugriff auf persönliche Daten durch die Lehrkraft. Hierbei müssen datenschutzrechtliche Anforderungen bedacht werden. Eine Benutzerordnung hilft Schülern und Eltern über diesen Sachverhalt zu informieren.

6. Machen Sie sich bitte Gedanken zum Thema **(Client-)Security**. Computernetzwerke mit vielen Benutzern bieten mannigfaltige Gelegenheiten für das Ausbreiten von Malware. Ein unbedachter Download, ein infizierter USB-Stick, ein infizierter Anhang einer E-Mail,... Die Möglichkeit der

[9] Ein Beispiel einer Nutzungsordnung finden Sie unter http://lehrerfortbildung-bw.de/sueb/recht/form/netz/

Computerrestauration sorgt zwar dafür, dass Rechner wieder desinfiziert werden, bis zum Erkennen und Beseitigen einer Infektion, kann diese jedoch weitere Systeme befallen. Manche Schadprogramme verbreiten sich auch automatisch über das Netzwerk und befallen die Homeverzeichnisse aller Benutzer, die sich zum Zeitpunkt der Infektion angemeldet haben. Wir wollen hier keine Panik verbreiten, Sie aber dennoch darauf hinweisen, dass der **Einsatz eines Virenscanners** durchaus Sinn ergibt und die Arbeit für die Einrichtung eines Schutzprogrammes den Aufwand für die Beseitigung einer Infektion locker wett macht.

Es gibt ein opsi-Paket „*clamav-win*“, das einen rudimentären Basisschutz bietet.

Bitte lassen Sie sich zu diesem Thema von Ihrem Hardwarehändler beraten.

7. Im Zusammenhang mit Sicherheitsüberlegungen müssen wir natürlich auch das **Sperren von USB-Sticks** in den Blick nehmen. Aus Sicherheitsgründen ist es im Auslieferungszustand für Schüler nicht möglich auf Wechseldatenträger zuzugreifen. Dieser Zugriff kann aber aus bestimmten Gründen doch Sinn ergeben (Daten für Präsentationen in das Netzwerk bringen, Sicherung von Benutzerdaten,…). Hierbei gilt es Schaden und Nutzen abzuwägen (siehe oben). Die Deaktivierung der Sperre externer Speichermedien ist in Kapitel 12.4, ab Seite 193 beschrieben.

2. Unterrichtsorganisation und -steuerung

Unter dem Hauptmenü *UCS@school Unterricht* stehen Ihnen als Netzwerkberater die gleichen Werkzeuge für die Gestaltung des Unterrichts zur Verfügung, auf die alle Lehrkräfte nach Anmeldung an der *Schulkonsole* zugreifen können. Da die Unterrichtsorganisation ausführlich im Lehrerhandbuch der paedML Linux beschrieben wird, möchten wir Sie für die Beschreibung der Funktionen der Unterrichtswerkzeuge auf dieses Handbuch verweisen.

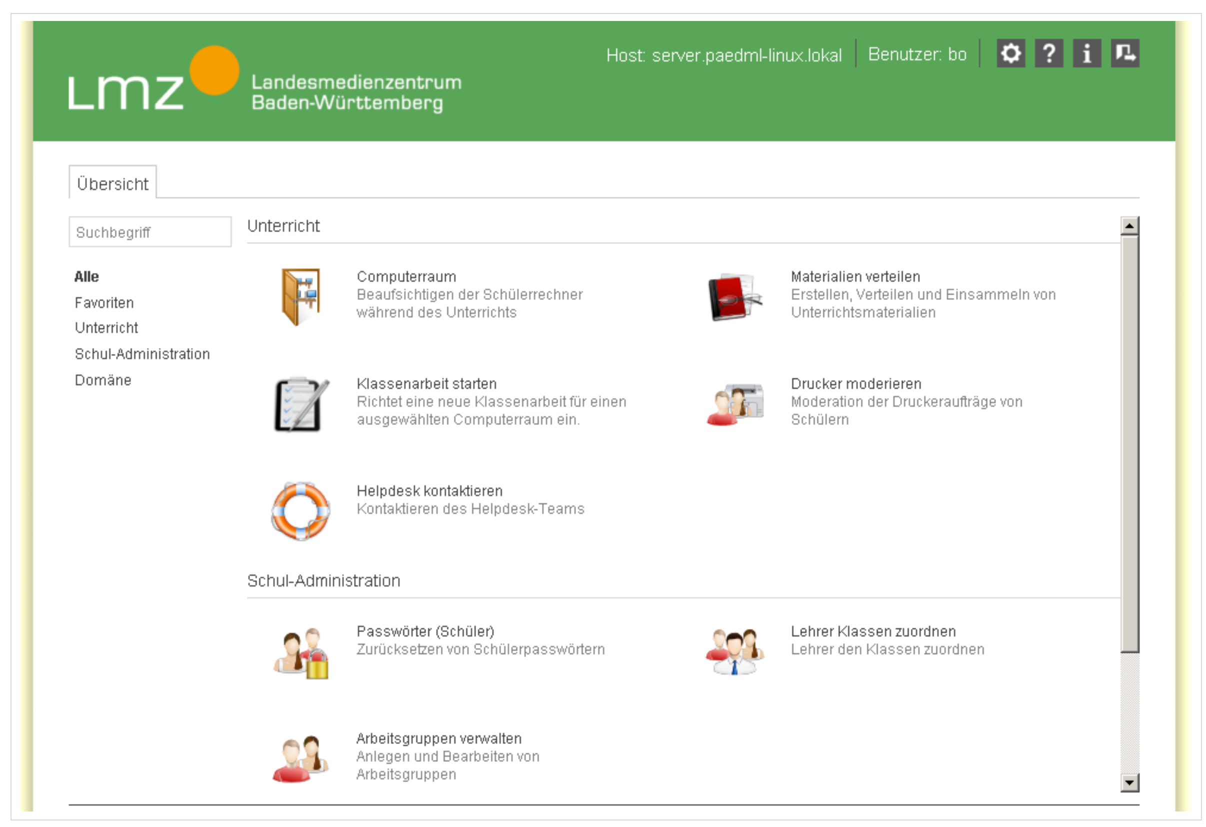


Abb. 19: Schöner unterrichten mit der Schulkonsole.

3. Benutzerverwaltung



Bitte beachten Sie unbedingt die Hinweise zur Nomenklatur der *paedML Linux* im Anhang A, Seite 295.



Beim Anlegen und Versetzen von Benutzern laufen im Hintergrund verschiedene Prozesse ab, über die Daten zwischen dem LDAP-Verzeichnis und Samba synchronsiert werden. Der Fortschritt der Datensynchronisation wird nicht an der *Schulkonsole* angezeigt.

Warten Sie nach dem Ausführen von Änderungen einige Zeit ab, bis Sie weitere Änderungen an Benutzerdaten vornehmen. Das System verarbeitet pro Stunde ca. 800 Benutzerdaten.

Der Fortschritt der Datensynchronisation kann an der Konsole des Servers mit dem Befehl

```
# tailf /var/log/univention/connector-s4.log
```

Eingesehen werden. Wenn hier keine Änderungen mehr vorgenommen werden, ist die Synchronisation abgeschlossen.

Übersicht

Dieses Kapitel beschreibt den Umgang mit Benutzern in der *paedML Linux 6.0*.

- Zunächst betrachten wir den Import von Benutzerlisten, durch die Sie Benutzer in die paedML Linux einpflegen.
- Kapitel 3.2 (ab Seite 54) beschreibt, wie Sie Schüler versetzen.
- Kapitel 3.3 (ab Seite 54) erklärt, wie Sie Datensätze überprüfen und ggf. modifiziert können.
- Kapitel 3.4 (ab Seite 56) erläutert das manuelle Hinzufügen einzelner Benutzer.
- Es folgt ein kurzer Überblick über das Löschen von Benutzern (Kapitel 3.5, ab Seite 58).
- Das Ändern von Kennwörtern wird in Kapitel 3.6 behandelt, die Passwort-Policy (also das Regelwerk der paedML Linux-Passwörter) ist Gegenstand in Kapitel 3.7.
- Das Kapitel zur Benutzerverwaltung endet mit einem Verweis auf das Handbuch für Lehrkräfte, in dem der Umgang mit Arbeitsgruppen beschrieben wird (Seite 63).

3.1 Import von Benutzerlisten über die Schulkonsole

Aufruf über Schulkonsole (Administrator): Schul-Administration | CSV-Import
Die Benutzerverwaltung der *paedML Linux* ist darauf ausgelegt, dass die primäre Verwaltung der Schülerdaten durch die Schulverwaltung erfolgt. Diese Daten werden in eine Datei im CSV-Format exportiert und in die *paedML* importiert.

Die Verarbeitung von Nutzerdaten der *paedML Linux* erfolgt über die Schulkonsole. Über das Schulkonsolenmodul „*Schul-Administration* | *CSV-Import*“ werden sowohl Lehrer als auch Schülerlisten eingelesen.

Hierbei können Sie auch Benutzerlisten aus Ihrer Vorgängerversion der *paedML Linux* übernehmen.

Schon bei den Vorgängerversionen der *paedML Linux* war die Verwaltung der Daten von Schülern und Lehrern in verschiedenen Listen aufgeteilt. Dieses Verfahren muss weiterhin praktiziert werden.

Vom Server werden beim Anlegen von Benutzern die folgenden Schritte ausgeführt:

- Anlage von LDAP-Datensatz des Benutzers. Die Daten hierfür werden aus der Benutzerliste/ Schulkonsole importiert. Mit Hilfe der Login-Daten (Benutzername und Kennwort) kann sich ein Benutzer im schulischen Netzwerk anmelden.
- Es wird ein Benutzername generiert.
- Es wird ein Passwort generiert.
- Neu angelegte Benutzer bekommen eine interne Mailadresse (BENUTZERNAME@paedml-linux.lokal).

  AUSNAHME: Benutzer mit Sonderzeichen im Namen bekommen keine Mailadresse generiert. Die Mailadresse bei diesen Benutzern muss manuell angelegt werden.
- Mit der ersten Anmeldung eines Benutzers im Netzwerk wird sein „Homeverzeichnis“ angelegt, in dem die Daten des Benutzers (Dokumente, *Windows*-Benutzerprofil,...) gespeichert werden.
  - Verzeichnisname bei Lehrern: */home/lehrer/ BENUTZERNAME*
  - Verzeichnisname bei Schülern: */home/schueler/BENUTZERNAME*

3.1.1 Format der Benutzerlisten

Für den Import von Schülerlisten können Sie sich eine Datei aus dem Schulverwaltungsprogramm exportieren lassen, in der alle Schüler eingetragen sind.

Diese Datei sollte UTF-8 kodiert sein. Jede Zeile dieser Datei enthält einen Benutzerdatensatz. **Die einzelnen Felder der CSV-Datei sind durch ein Semikolon zu trennen**.

Die Dateien dürfen KEINE Leezeichen oder Tabulatoren enthalten.

Die Datensätze der Benutzerlisten haben verschiedene Felder, die befüllt werden können. Die folgenden Felder sind verfügbar:

Datentyp des Feldes	Hinweise
Klasse	▪ Hier kann ein alphanumerischer Wert eingetragen werden (z.B. 7a, gym-9c) ▪ Geben Sie bei Schülern einen Wert für die Klasse ein. Die Schüler werden beim Anlegen an die Gruppe der Klasse zugewiesen. ▪ Beim Versetzen von Schülern wird der Wert im Feld Klasse geändert. ▪ Lehrer tragen sich später über die Schulkonsole in Klassen ein. Hier kann als Platzhalter die Klasse „Lehrer“ eingetragen werden.
Nachname	▪ Umlaute und das scharfe S (ß) werden beim Import von Benutzern vom System verarbeitet.

	▪	Achten Sie darauf, dass keine Sonderzeichen (?, !, ..) Accents oder ähnliches in den Benutzernamen vorkommen dürfen.
	▪	Die Zeichenlänge von Benutzernamen sollte auf 15 Zeichen beschränkt werden, sofern Sie den Klassenarbeitsmodus nutzen wollen. Hierfür müssen der Import-Liste Benutzernamen mitgegeben werden.
Vorname	▪	siehe Nachname
Benutzername	▪	Der Benutzername wird automatisch generiert. Dabei werden jeweils die Benutzernamen „VORNAME.NACHNAME“ angelegt.
	▪	Sie können auch eigene Benutzernamen definieren.
	▪	Wenn Benutzer den gleichen Vor- und Nachnamen haben, dann werden beide Datensätze rot hinterlegt (s.u.). Für einen der Benutzer muss in diesem Fall händisch der Benutzername angelegt werden. Wir empfehlen, den Namen „*VORNAME.NACHNAME1*“ zu vergeben.
	▪	Beschränken Sie den Benutzernamen immer auf 15 Zeichen.
Geburtstag	▪	Format: TT.MM.JJJJ (z.B. 24.12.1993)
	▪	Geburtsdaten müssen in der Vergangenheit liegen, jedoch nicht vor 1900.
E-Mail	▪	Mailadressen werden automatisch generiert (BENUTZERNAME@paedml-linux.lokal)
	▪	Bei Benutzern mit Sonderzeichen im (Benutzer-) Namen muss die Mail-Adresse manuell angelegt werden, da Benutzer mit Sonderzeichen derzeit keine automatische Mailadresse bekommen.
Passwort	▪	Wenn hier kein Eintrag vorgenommen wird, dann wird jedem Benutzer ein vom System generiertes, nicht auslesbares Passwort gesetzt. An der Schulkonsole können die Passwörter später geändert werden (vgl. Kapitel 3.6, Seite 60).

Tabelle 6: Felder für den CSV-Import.



Sie müssen nicht alle Felder zuweisen. Aus den „führenden“ Feldern Vor- und Nachname wird ein Benutzerdatensatz generiert. Die anderen Felder sind zwar optional, es sollte aber mindestens noch die Klasse der Schüler angegeben werden.

Beispiel einer Schülerliste:

```
(…)
7B;Jupp;Heynckes;09.05.1945
7B;Bernd;Hölzenbein;09.03.1946
8A;Gerd;Müller;03.11.1945
(…)
```

Die Lehrerliste kann folgendermaßen aufgebaut sein[10]:

```
(…)
Lehrer;Hans;Bo;01.03.1902;bo
Lehrer;Heinz;Bader;03.01.1908;ba
(…)
```

Übertragen Sie die Benutzer-Listen auf die *Admin-VM*. Erstellen Sie ein Verzeichnis „*Benutzer-Listen*“ auf dem Desktop. Kopieren Sie die Benutzerlisten in dieses Verzeichnis. Die empfohlenen Dateinamen lauten „*lehrer.csv*“ und „*schüler.csv*“.

Die Hotline kann im Fehlerfall einfacher auf die Dateien zugreifen, wenn Sie sich an diese Namensvorgaben halten, da die Listen nicht gesucht werden müssen.

3.1.2 Stichwort: „Datenkonsistenz“



Überprüfen Sie vor dem Import alle Benutzerlisten auf ihre Richtigkeit. Dies erspart Ihnen Arbeit, die Sie mit für das Nachbessern von Fehlern aufwenden müssen.

Achten Sie insbesondere darauf, dass alle Spalten der Benutzerlisten richtig angelegt wurden. Ein Geburtsdatum in der Spalte der Nachnamen sorgt zum Beispiel dafür, dass der Schüler *Vorname.Geburtsdatum* angelegt wird!

Die Reihenfolge der Felder der csv-Dateien ist zunächst nicht wichtig, wobei die Dateien in sich natürlich konsistent sein sollten. Die Datentypen der Felder werden beim Import über die Schulkonsole zugewiesen.

Achten Sie beim Import neuer Benutzerlisten unbedingt auf Datenkonsistenz!

Die Benutzerverwaltung der paedML Linux ist so konfiguriert, dass die Datensätze der Benutzer vor dem Anlegen überprüft werden. Wenn in den Daten eines bestehenden Benutzers Änderungen vorgenommen werden, wird der alte Datensatz (inklusive Benutzerkonto) unter Umständen gelöscht und ein neuer Benutzer angelegt.

Es erfolgt eine Sicherung der alten Benutzerdaten nach */home/backup/ALTERBENUTZERNAME*

Wenn Benutzer manuell an der Schulkonsole angelegt wurden (vgl. Kapitel 3.4, Seite 56) müssen die Daten dieser Benutzer mit der Liste des Schulverwaltungs-Programmes abgeglichen werden.

Obgleich in der Praxis vermutlich nicht umsetzbar, wäre ein Informationsfluss zwischen Sekretariat und Netzwerkberater bezüglich geänderter Stammdaten von Benutzern (Korrektur von Schüler-Namen,…), hilfreich.

Hierdurch könnten geänderte Schüler beim Import neuer Listen schneller identifiziert und ggf. der jeweilige Datensatz angepasst werden, bevor der Schüler versehentlich gelöscht und neu angelegt wird.

[10] Der Eintrag „Lehrer“ ist ein Platzhalter. Später können sich Lehrkräfte selbst in Klassen ein- und austragen.

Das Ändern von Datensätzen an der Schulkonsole ist zwar möglich, es besteht jedoch auch hier die Gefahr, dass Änderungen nicht in das Schulverwaltungsprogramm, bzw. in die Benutzerlisten übertragen werden und Benutzer gegebenenfalls gelöscht und neu angelegt werden. Wir raten daher den Benutzer-Import ausschließlich über Benutzerlisten vorzunehmen.

Beim Import der Listen müssen ALLE zu importierenden Felder ALLER Benutzer durchgängig mit den gleichen Datentypen befüllt sein.

Ein Beispiel einer „falschen" Lehrerliste:

```
(…)
JG-2,5b,9c;Heinz;Bader;03.01.1908;ba
Hans;Bo;01.03.1902;bo
Sorglos;Siegfried;13.08.1911
(…)
```

Aus diesem Beispiel können Sie herauslesen, dass der automatische Import fehlschlagen muss!

1. Der Datensatz von Heinz Bader ist der einzige „richtige" Datensatz, in dem alle Felder sauber belegt sind.
2. Bei Hans Bo gibt es keine Klassen, wodurch beim Anlegen alle Datenfelder verrutschen würden.
3. Siegfried Sorglos hat weder eine Klassen-Zuordnung noch einen Login-Namen. Der Vor- und Nachname sind bei diesem Datensatz vertauscht.

Klasse	Vorname	Nachname	Geburtstag	Benutzername
JG-2,5b,9c	Heinz	Bader	03.01.1908	ba
Hans	Bo	01.03.1902	bo	
Sorglos	Siegfried	13.08.1911		

Abb. 20: Dieser Datenimport führt zu einem unbrauchbaren Ergebnis!

Nach der Auswertung der Import-Liste zeigt das System Ergebnisse, die Sie guten Gewissens verwerfen sollten. In diesem Fall muss die CSV-Datei, auf der der Import basiert, nochmals überarbeitet werden.

☐	Aktion	Klasse	Vorname	Nachname	Geburtstag	Benutzername	Zeile
☐	Erstellen	JG-2, 5b, 9c	Heinz	Bader	03.01.1908	ba	1
☐	Erstellen	Hans	Bo	01.03.1902	bo	bo.01.03.1902	2
☐	Erstellen	Sorglos	Siegfried	13.08.1911		siegfried.13.08.1911	3

Abb. 21: Das Ergebnis dieses Imports ist unbrauchbar!

Wenn Werte leer gelassen werden sollen, müssen Sie mit einem Semikolon (;) übersprungen werden. Andernfalls „verrutschen" die Daten eines Datensatzes und der Datensatz wird falsch vom System eingelesen.

Das folgende Beispiel zeigt, wie fehlende Daten aufgefangen werden können (grüner Datensatz) und wie Fehler entstehen (roter Datensatz).

```
(Klasse;    Nachname;    Vorname;    Benutzername;      Geburtstag)
7B;         Heynckes;    Jupp;       Jupp.Henckes       09.05.1945
8A;         Müller;      Gerd;       ;                  03.11.1945
7B;         Hölzenbein;  Bernd;                         09.03.1946
```

3.1.3 Import der Benutzerlisten



Das Anlegen von Lehrer- und Schülerlisten geschieht nach den gleichen Mechanismen. Wir beschreiben nur das Verfahren für Schüler. Unterschiede zwischen diesen beiden Gruppen bestehen lediglich in folgenden Punkten: Lehrkräfte haben mehr Berechtigungen. Schüler gehören immer nur einer Klasse an, während Lehrer verschiedenen Klassen zugewiesen werden können.

Um eine Benutzerliste in das System zu übernehmen, öffnen Sie die Schulkonsole und darin den Menüpunkt „*Schul-Administration* | *CSV-Import*".

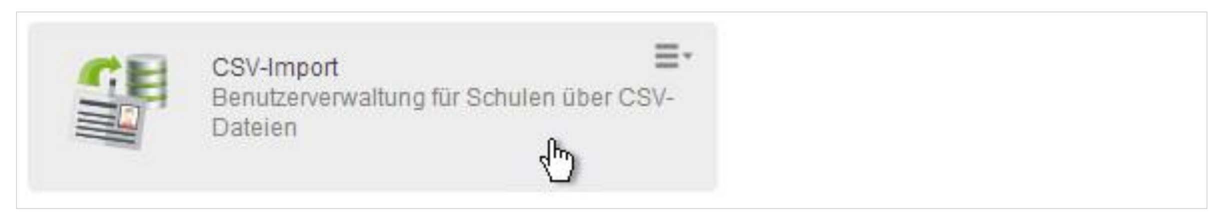


Abb. 22: Der Knopf „CSV-Import bringt Sie zum Benutzer-Import.

Im ersten Dialog treffen Sie die Auswahl, ob Lehrer oder Schüler in das System übernommen werden sollen. Achten Sie auf die richtige Auswahl! Wählen Sie die Benutzerrolle, die den Einträgen der Liste zugeordnet werden soll und drücken Sie anschließend „*Weiter*", um fortzufahren.

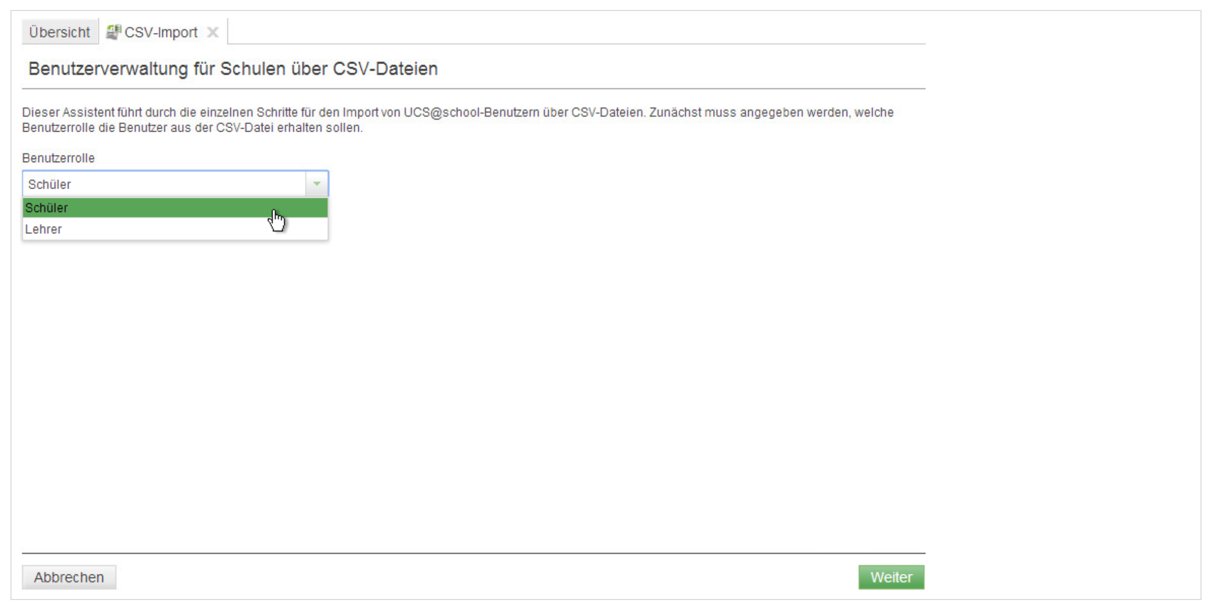


Abb. 23: Auswahl: Welche Art von Benutzern sollen importiert werden?

Die nächste Maske ermöglicht Ihnen, eine CSV-Datei auszuwählen. Drücken Sie hierfür den Knopf „*Hochladen*“ und wählen Sie die zu importierende Liste. Überprüfen Sie, ob Sie den Haken vor „*Austausch der vorhandenen Benutzer…*“ setzen und fortfahren wollen.



Wenn der Haken vor „*Austausch der vorhandenen Benutzer…*“ gesetzt ist, werden alle nicht mehr in der Liste vorhandenen Benutzer gelöscht.

Dies kann gewünscht sein, wenn Sie beim Schuljahreswechsel alte Schüler aus dem System löschen wollen.

Wenn der Haken beim Einpflegen einer Liste mit ausschließlich neuen Schülern zur Jahresmitte gesetzt ist, wäre das Löschen der restlichen Schüler verheerend!



Abb. 24: Auswahl der Import-Liste.

Sobald die Liste in das System geladen wurde, bekommen Sie eine Maske, in der Sie den Spalten die jeweiligen Datentypen zuweisen müssen. Klicken Sie hierfür oberhalb jeder Spalte auf den Eintrag „*Unbenutzt*“. Es öffnet sich eine Liste mit Werten, die Sie den Spalten zuweisen können. Übernehmen Sie die Auswahl mit „*Weiter*“.

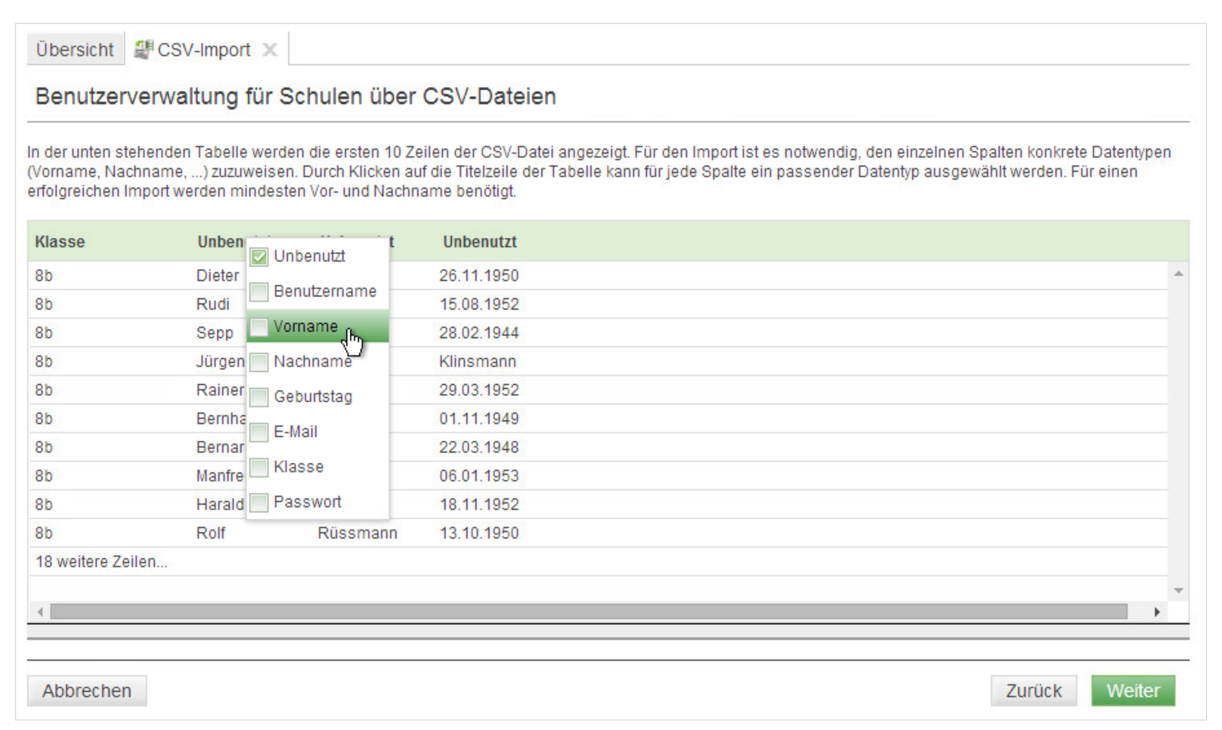


Abb. 25: Zuweisung von Datentypen an die Spalten der Benutzerliste

Sofern Sie keine Spalte „*Benutzername*“ definiert haben, erscheint der folgende Dialog. Klicken Sie auf „*Benutzernamen automatisch bestimmen*“, um durch das System Benutzernamen „*Vorname.Nachname*“ generieren zu lassen.

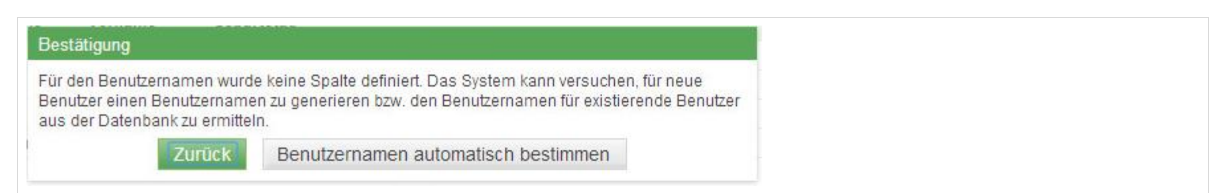


Abb. 26: Automatisches Anlegen von Benutzernamen?

Im folgenden Schritt werden alle Datensätze überprüft. Dabei werden folgende Entscheidungen vom System getroffen:

Situation	**Aktion**
Benutzer sind neu in der Benutzerliste.	„*Erstellen*“ der Benutzer
Benutzer sind nicht mehr in der Benutzerliste.	„*Löschen*“ der Benutzer
Vorhandene Benutzer werden in andere Klassen versetzt.	„*Ändern*“ der Benutzer

Tabelle 7: Aktionen des CSV-Import-Skriptes.

Gleichzeitig überprüft das System, ob die übergebenen Datensätze plausibel sind.

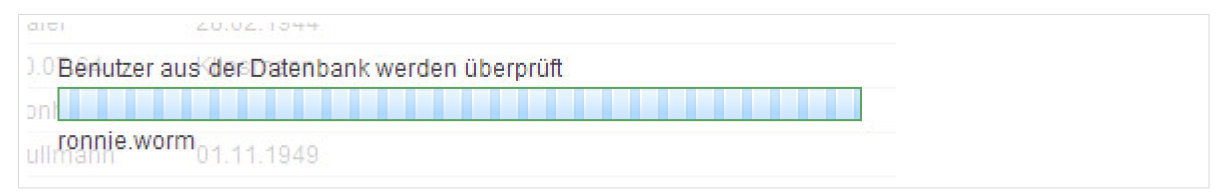


Abb. 27: Überprüfen der Benutzerdaten.

Bevor die Benutzer im folgenden Schritt in das System eingepflegt werden, erhalten Sie eine Ausgabe aller vom System überprüften Datensätze der CSV-Datei.

3.1.3.1 Korrektur fehlerhafter Datensätze

Vom System als fehlerhaft erkannte Datensätze werden rot hervorgehoben. Wenn Sie die Ansicht auf diese Datensätze beschränken wollen, dann klicken Sie auf die Checkbox vor *„Nur Zeilen mit Problemen anzeigen*".

Benutzerverwaltung für Schulen über CSV-Dateien

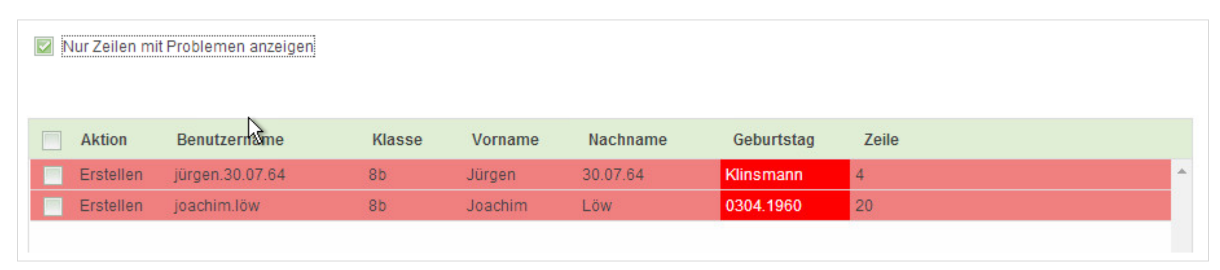
Die CSV-Datei wurde mit dem vorhandenen Datenbestand abgeglichen. In der Tabelle werden die einzelnen Benutzeränderungen angezeigt, wobei Probleme farblich hervorgehoben werden. Die einzelnen Zeilen können über die Schaltfläche "Bearbeiten" oder über einen Klick auf den Wert in der Spalte "Aktion" bearbeitet werden.

Nur Zeilen mit Problemen anzeigen

Aktion	Benutzername	Klasse	Vorname	Nachname	Geburtstag	Zeile
Ändern	dieter.burdenski	8b	Dieter	Burdenski	26.11.1950	1
Ändern	rudi.kargus	8b	Rudi	Kargus	15.08.1952	2
Ändern	sepp.maier	8b	Sepp	Maier	28.02.1944	3
Erstellen	jürgen.30.07.64	8b	Jürgen	30.07.64	Klinsmann	4

Abb. 28: Ausgabe der überprüften Benutzerliste.

In fehlerhaften Datensätzen wird hervorgehoben, welche Probleme erkannt wurden. Im folgenden Screenshot gibt es Fehler bei den Geburtstagen der Benutzer. Der Benutzername *„jürgen.30.07.64*" zeigt außerdem, dass eine erneute Überprüfung der Benutzerlisten in diesem Stadium durchaus Sinn ergibt.



Nur Zeilen mit Problemen anzeigen

Aktion	Benutzername	Klasse	Vorname	Nachname	Geburtstag	Zeile
Erstellen	jürgen.30.07.64	8b	Jürgen	30.07.64	Klinsmann	4
Erstellen	joachim.löw	8b	Joachim	Löw	0304.1960	20

Abb. 29: Die Ausgabe wurde auf fehlerhafte Datensätze beschränkt.

Es findet zusätzlich ein Abgleich mit den Daten bestehender Benutzer statt. Differenzen zwischen den im System hinterlegten Daten und den Daten der aktuellen Import-Liste werden gelb hervorgehoben. Im folgenden Screenshot wurde das Geburtsdatum geändert. Bei Übernahme dieser Änderung wird der Geburtstag des Benutzers geändert.

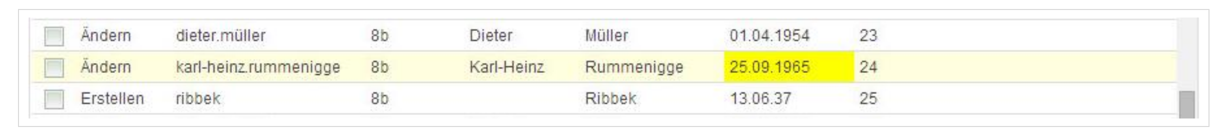


Abb. 30: Differenzen zwischen bestehenden Daten und neuer Import-Liste.

Um einen zu ändernden Datensatz zu bearbeiten, klicken Sie mit Doppelklick (linke Maustaste) auf den Datensatz. Im nächsten Dialog können Sie den Datensatz korrigieren. Beenden Sie die erfolgreiche Bearbeitung durch einen Klick auf „*Übernehmen*“.

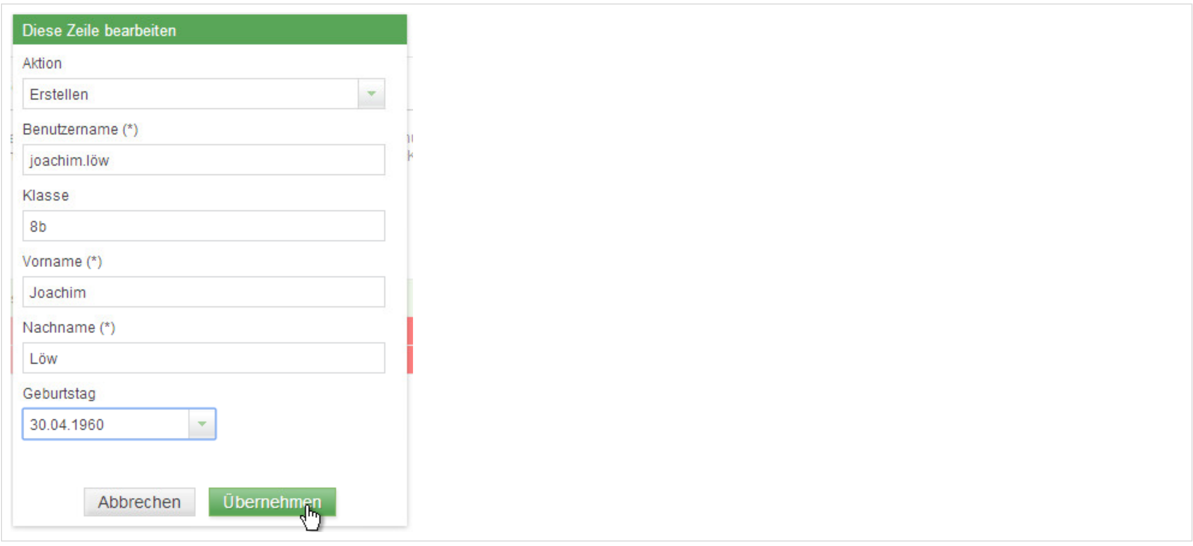


Abb. 31: Ändern eines fehlerhaften Datensatzes.

Nach der Korrektur der falschen Daten wird der Datensatz als „richtig“ erkannt. Die Auswahl kann durch Entfernen des Hakens vor „*Nur Zeilen mit Problemen anzeigen*“ wieder auf alle Datensätze erweitert werden.



Abb. 32: Datensätze können vor dem Import in der Schulkonsole korrigiert werden.

3.1.4 Sortieren

Das CSV-Import-Modul bietet die Möglichkeit die Datensätze nach einer bestimmten Spalte sortieren zu lassen. Am interessantesten dürfte hierbei das Sortieren nach den Einträgen der Spalte „*Aktion*“ sein. Klicken Sie auf eine Spaltenüberschrift, um die Tabelle nach der Spalte zu sortieren. Drücken Sie erneut auf die Überschrift, um die Sortierreihenfolge umzudrehen.

Im folgenden Screenshot wurde nach „Aktion“ sortiert. Dadurch werden alle Benutzer gruppiert, deren Daten einer bestimmten Aktion zugeordnet wurden. **Nutzen Sie Ihre letzte Chance, um zu überprüfen, ob die Daten korrekt sind!**



Aktion	Benutzername	Klasse	Vorname	Nachname	Geburtstag	Zeile
Erstellen	jürgen.30.07.64	8b	Jürgen	30.07.64	Klinsmann	4
Erstellen	rudi.völler	8b	Rudi	Völler	13.04.60	13
Erstellen	joachim.löw	8b	Joachim	Löw	30.04.1960	20
Erstellen	ribbek	8b		Ribbek	13.06.37	25
Löschen	ronnie.worm	8b	Ronnie	Worm	07.10.1953	
Ändern	bernhard.cullmann	8b	Bernhard	Cullmann	01.11.1949	6
Ändern	bernard.dietz	8b	Bernard	Dietz	22.03.1948	7
Ändern	manfred.kaltz	8b	Manfred	Kaltz	06.01.1953	8

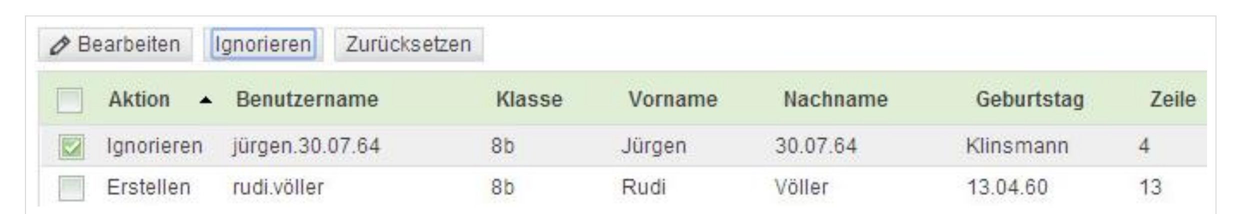
Abb. 33: Sortieren der Benutzerliste nach „Aktion“.

3.1.5 Ignorieren

Datensätze, bei denen Sie sich nicht sicher sind, ob diese importiert werden sollen, können nun vom Import ausgenommen werden, in dem Sie zuerst die Checkbox vor den betreffenden Daten aktivieren und anschließend auf „*Ignorieren*“ klicken. Der Eintrag im Feld „Aktion“ der ausgewählten Datensätze wird ebenfalls mit dem Wert „*Ignorieren*“ befüllt. Diese Datensätze werden nicht in das System übernommen.



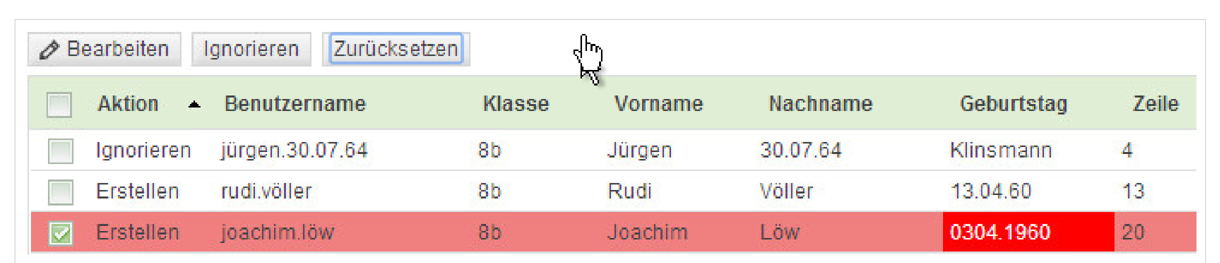
Notieren Sie sich alle Datensätze, die Sie vom Import ausschließen, damit Sie diese zu einem späteren Zeitpunkt in das System einpflegen können.



Aktion	Benutzername	Klasse	Vorname	Nachname	Geburtstag	Zeile
Ignorieren	jürgen.30.07.64	8b	Jürgen	30.07.64	Klinsmann	4
Erstellen	rudi.völler	8b	Rudi	Völler	13.04.60	13

Abb. 34: Ignorieren Fehlerhafter Datensätze.

Sie können Änderungen, die an der Schulkonsole getätigt wurden, rückgängig machen, indem Sie den Datensatz auswählen (Haken setzen) und die Taste „Zurücksetzen“ drücken.



Aktion	Benutzername	Klasse	Vorname	Nachname	Geburtstag	Zeile
Ignorieren	jürgen.30.07.64	8b	Jürgen	30.07.64	Klinsmann	4
Erstellen	rudi.völler	8b	Rudi	Völler	13.04.60	13
Erstellen	joachim.löw	8b	Joachim	Löw	0304.1960	20

Abb. 35: An der Schulkonsole vorgenommene Änderungen der Datensätze können rückgängig gemacht werden.

3.1.6 Importieren

Ein Klick auf „*Weiter*“ (unten rechts) übernimmt die Liste in das System, sofern alle Fehler bereinigt wurden. Wenn es noch fehlerhafte Datensätze gibt, dann wird eine Warnmeldung eingeblendet:



Abb. 36: Warnmeldung bei fehlerhaften Datensätzen.

Wenn alle Fehler behoben wurden, kann die Liste in das System eingespielt werden. In einem Dialogfenster wird angezeigt, welche Änderungen am System vorgenommen werden. Wenn diese Änderungen in Ordnung sind, können Sie mit „*Änderungen bestätigen*“ den Import der Benutzerliste anstoßen.

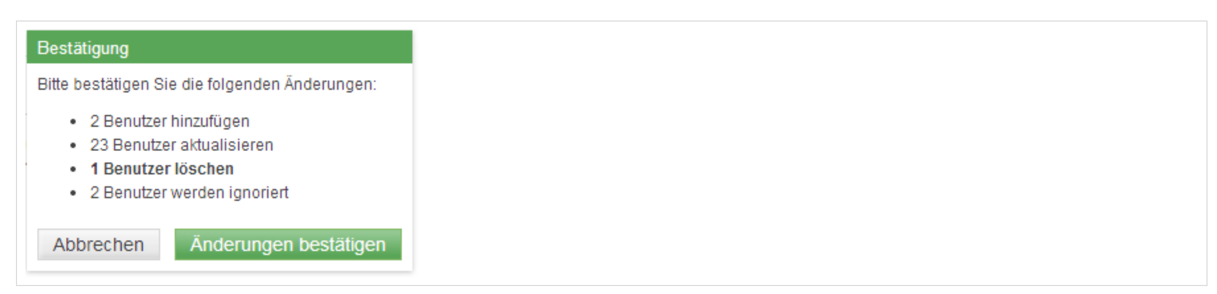


Abb. 37: Eine letzte Bestätigung und der Import läuft an.

Im Anschluss erfolgt die Verarbeitung der Datensätze,…

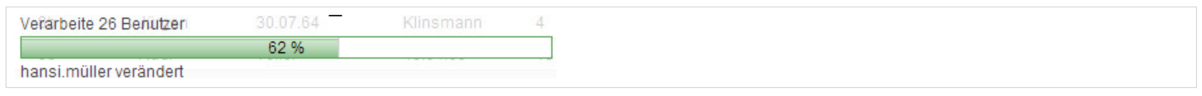


Abb. 38: Benutzerdaten werden verarbeitet…

… die im Idealfall keine Fehler liefern sollte. Im vorliegenden Fall hat das System beim Anlegen zwei fehlerhafte Geburtsdaten gefunden.

Diese Benutzer müssen nochmals gesondert überprüft und mit einer separaten Import-Liste dem System hinzugefügt werden.



Abb. 39: … und am Ende wird eine Ausgabe angezeigt.

Besser ist es natürlich, wenn keine Probleme auftreten:

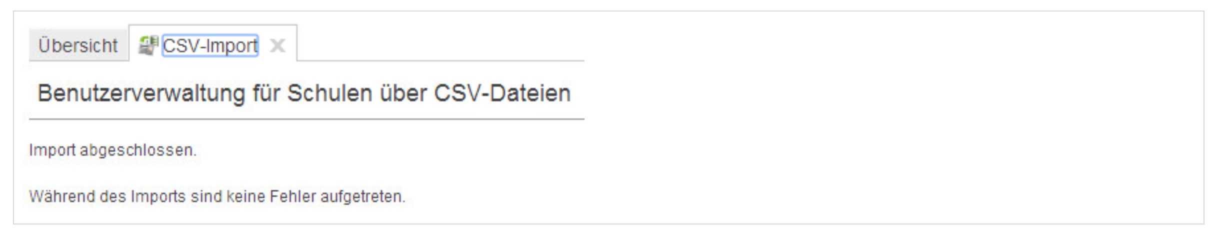


Abb. 40: Fehlerfreier Import

3.2 Versetzen von Schülern

Zum Schuljahreswechsel bekommen Sie eine neue CSV-Datei aus dem Schulverwaltungsprogramm, die Sie, wie im vorausgegangenen Kapitel beschrieben, in das System einpflegen.

Die Daten der Datei werden während des Prozesses überprüft und Benutzer werden – sofern sich sonst nichts am Stammdatensatz geändert hat – automatisch in eine neue Klasse versetzt.

3.3 Überprüfung und Modifikation von Benutzerdaten

Aufruf über Schulkonsole (Administrator): Schul-Administration | Benutzer (Schulen)
Der Benutzer Administrator kann sich alle Schüler und Lehrer, die in der paedML Linux angelegt sind, über das Schulkonsolenmenü „*Schul-Administration* | *Benutzer (Schulen)*“ anzeigen lassen.

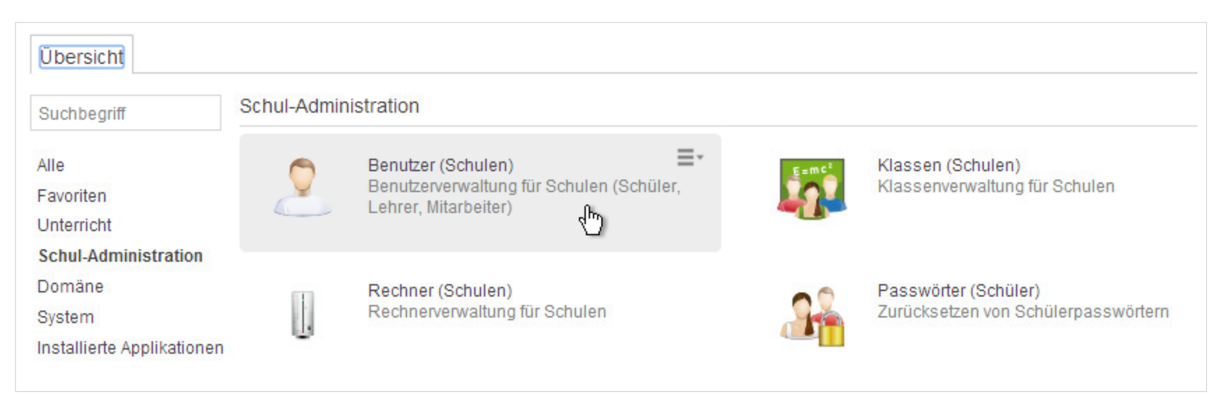


Abb. 41: Aufruf der Benutzerübersicht.

Beim Aufruf des Schulkonsolenmoduls werden alle verfügbaren Benutzer anzeigt. Sie können die Anzeige aber auch auf eine Systemrolle („*Schüler*“ oder „*Lehrer*“) einschränken oder durch einen Eintrag im Feld „*Filter*“ und einem anschließenden Klick auf „*Suchen*“ gezielt nach Anwendern suchen.

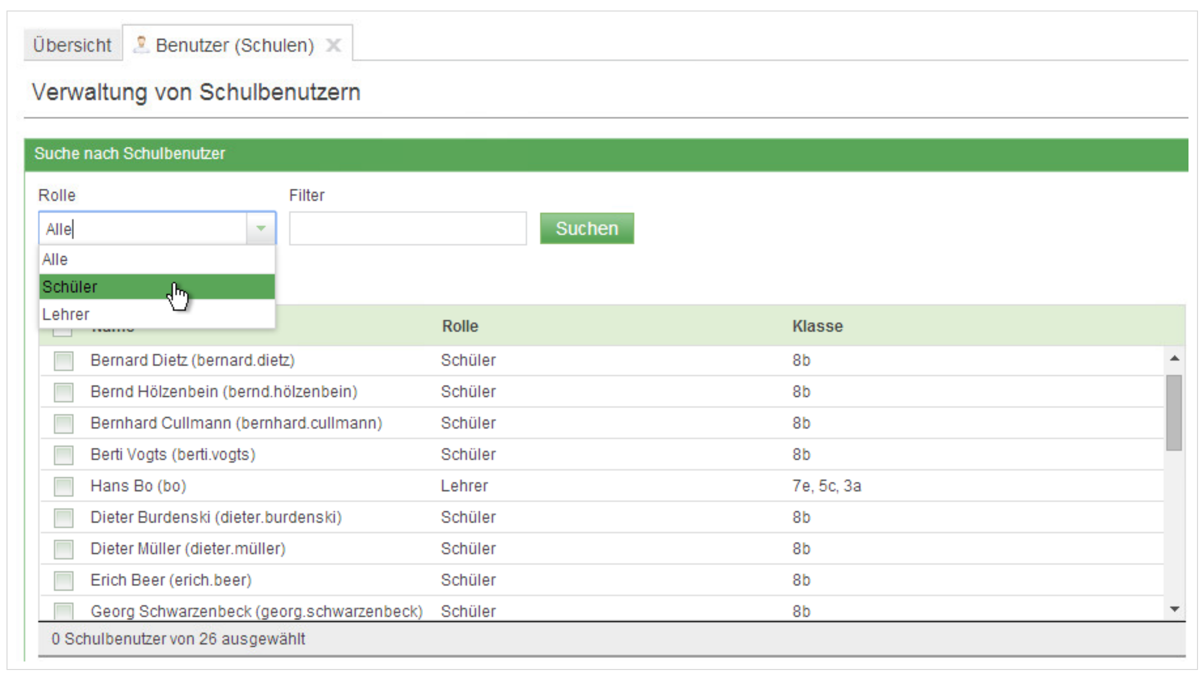


Abb. 42: Anzeige aller Anwender, die aber auch eingeschränkt werden kann.

Wenn Sie auf den Namen eines Benutzers drücken, dann öffnet sich eine Maske mit den Daten des Anwenders. Hier können Sie die Werte überprüfen und ggf. Änderungen vornehmen.

Nehmen Sie auf keinen Fall Änderungen unter „Erweiterte Einstellungen“ vor, da diese tief in das System reichen und nicht garantiert werden kann, dass der Benutzer weiterhin arbeiten kann.

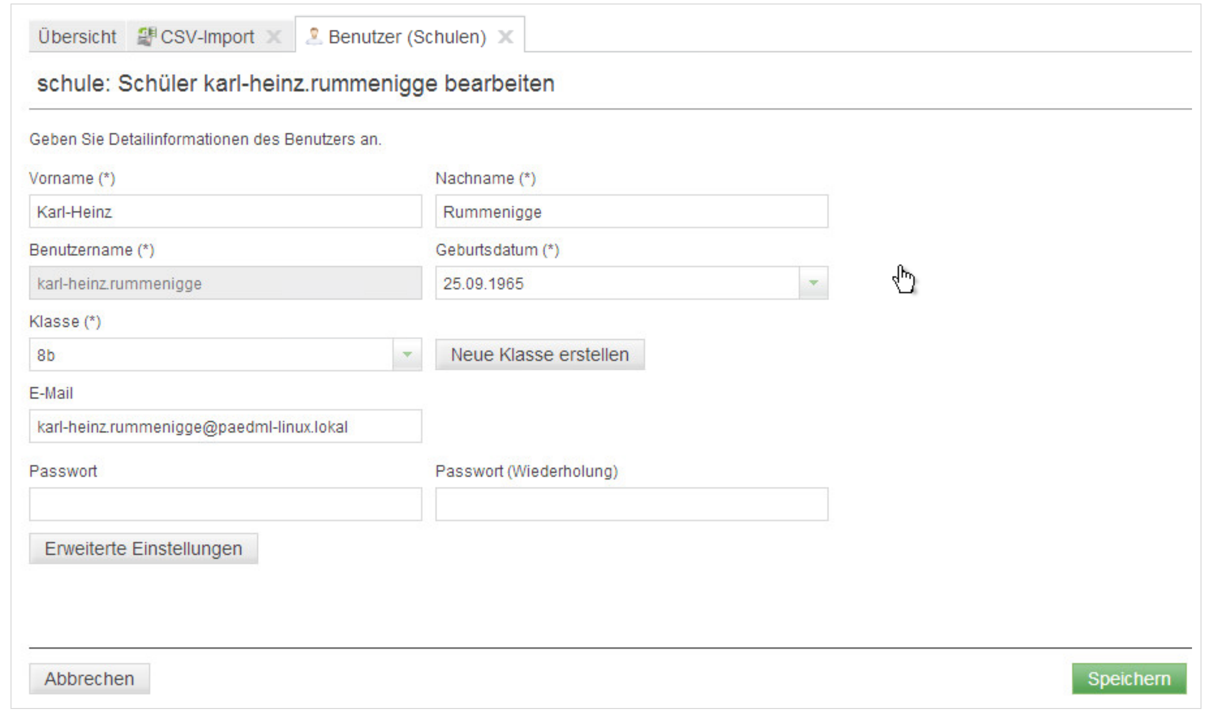


Abb. 43: Änderungsmaske von Benutzerdaten



Achten Sie auf Datenkonsistenz! Änderungen, die in diesem Modul vorgenommen werden, müssen in die Listen für das paedML-Import-Skript übertragen werden.

3.4 Anwender manuell hinzufügen



Wir empfehlen ausdrücklich, den Import von Benutzern über CSV-Dateien durchzuführen.

Im Einzelfall kann es sinnvoll sein, Benutzer über das hier beschriebene Verfahren manuell einzupflegen.

Ebenfalls im Schulkonsolenmenü „*Schul-Administration* | *Benutzer (Schulen)*“ finden Sie den Knopf „*Hinzufügen*“, über den Benutzer angelegt werden können.



Abb. 44: Hinzufügen einzelner Benutzer.

In der ersten Maske werden Sie gefragt, was für einen Benutzer Sie anlegen wollen. Wählen Sie einen Benutzertyp („Schüler“ oder „Lehrer“) und klicken Sie auf „*Weiter*“.

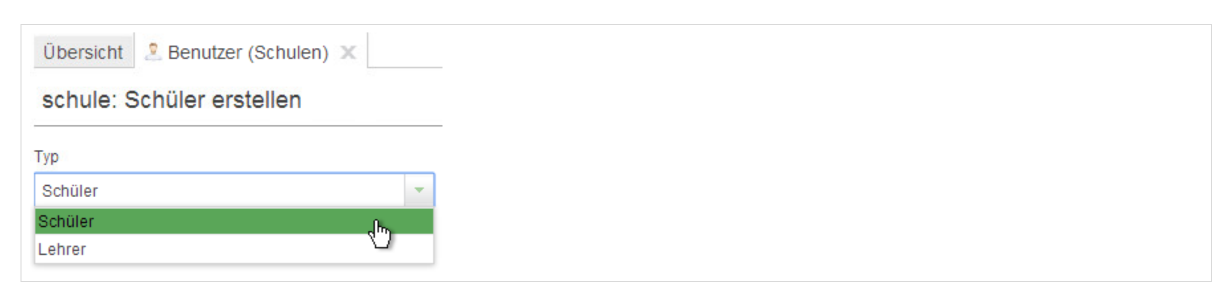


Abb. 45: Erster Schritt: Festlegen eines Benutzertyps.

Für das Anlegen von Benutzern benötigen Sie „*Vor- und Nachnamen*“, das „*Geburtsdatum*“ und einen „*Benutzernamen*“[11]. Optional können Sie den Benutzern noch eine „*E-Mail*“-Adresse zuweisen.

[11] Das Standardformat von Benutzernamen der paedML Linux ist vorname.nachname.

Die Masken für das Anlegen von Lehrern und Schülern unterscheiden sich im Feld „*Klasse*“. Dieses ist bei Schülern vorhanden und muss mit einem Wert befüllt werden.

Lehrer können sich – wie im „*Handbuch für Lehrkräfte*“ beschrieben – über die Schulkonsole einer Klasse zuordnen. Dies ergibt aus administrativer Sicht Sinn, da die Zuordnung sich regelmäßig ändern kann. Außerdem können Lehrer auch in Vertretungsstunden die „Kontrolle“ über Klassen übernehmen, beispielsweise um Unterrichtsmaterial an die Klasse verteilen zu können.



Das Feld „*Mailadresse*“ kann leer bleiben, sofern Sie den Benutzern keine Mailadresse vergeben wollen. In diesem Fall wird für den Benutzer kein Konto mit dem Benutzernamen im Mailsystem angelegt.



Wenn Sie kein Kennwort eingeben, dann wird ein Zufallskennwort vergeben.

Da es keine Möglichkeit gibt, dieses Kennwort auszulesen, empfehlen wir hier ein Kennwort zu setzen und dem Benutzer mitzuteilen.

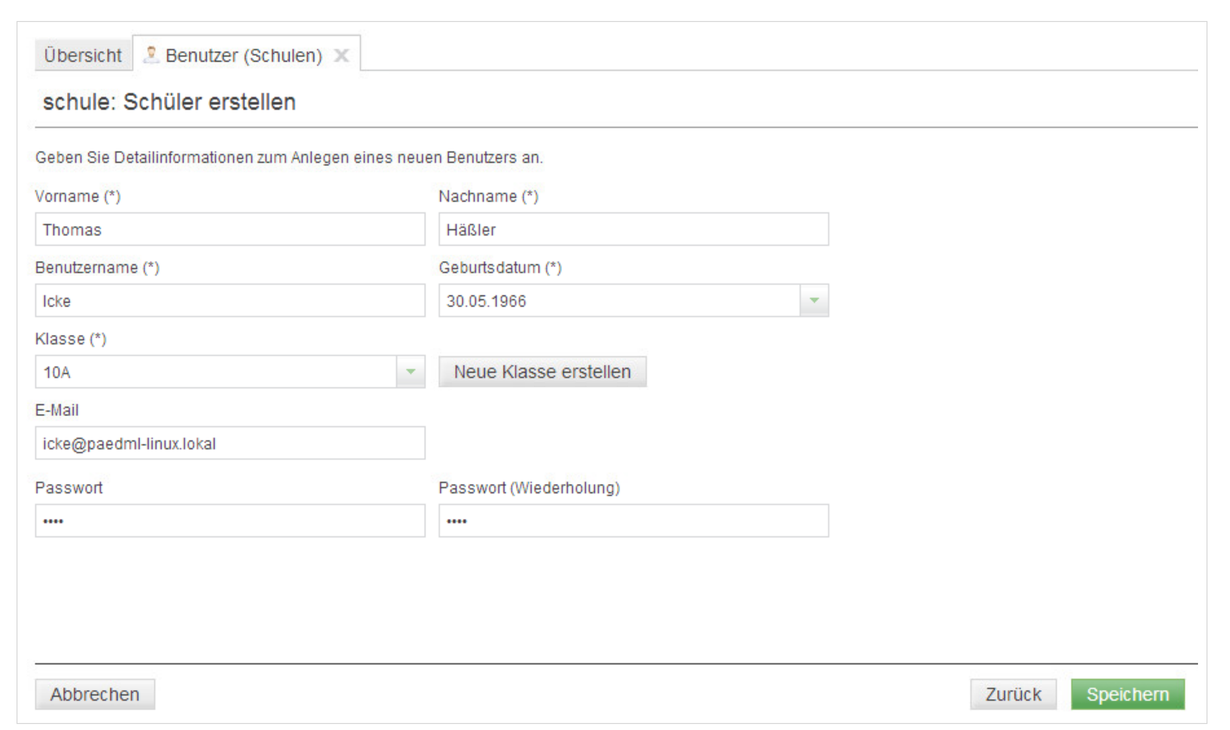


Abb. 46: Anlegen eines Schülers.

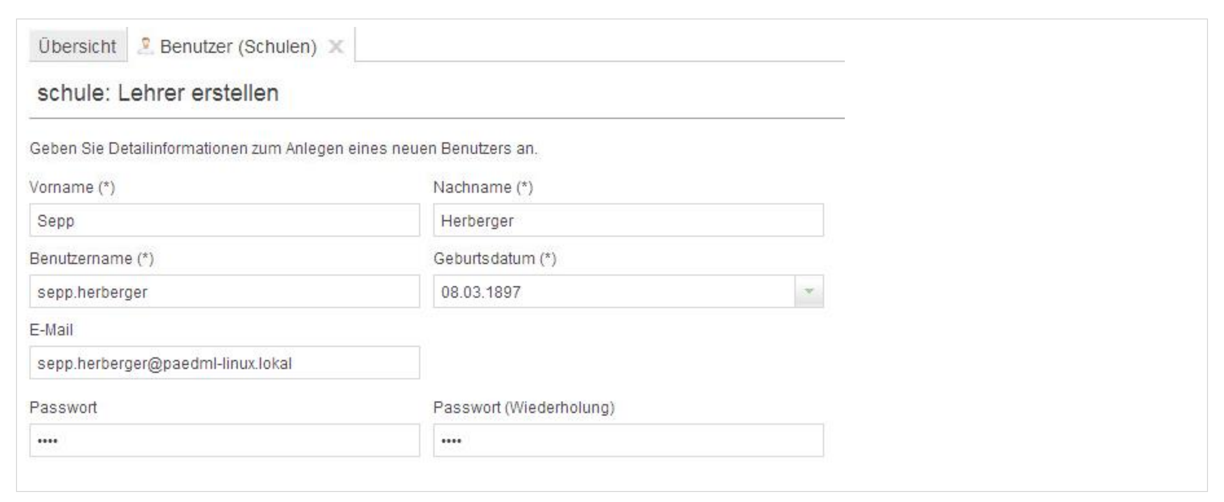


Abb. 47: Anlegen eines Lehrers mit lokalem Mailkonto.

Ein neu angelegtes Benutzerkonto wird mit einer Meldung im oberen Bereich des Browserfensters quittiert:

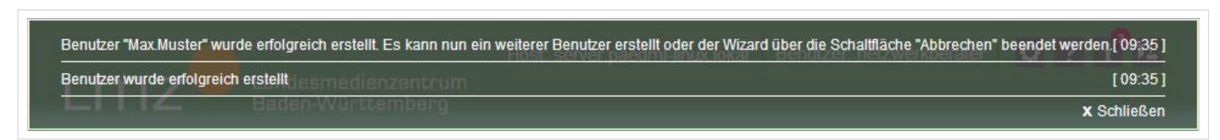


Abb. 48: Ein Benutzer wurde erfolgreich angelegt.

3.5 Benutzerdatensätze löschen

Aufruf über Schulkonsole (Administrator): Schul-Administration | Benutzer (Schulen)
Das Löschen angelegter Benutzer geschieht ebenfalls als Administrator im Menü „*Schul-Administration* | *Benutzer (Schulen)*“.



Der in dieser Maske vorhandene Benutzer „netzwerkberater“ darf unter keinen Umständen gelöscht werden.

Sollte dies doch versehentlich geschehen, müssen Sie an der Server-Konsole den Befehl

```
#lmz-settings-users
```

ausführen.

Markieren Sie alle Anwender, die Sie aus dem System löschen wollen und klicken Sie auf „*Löschen*“.

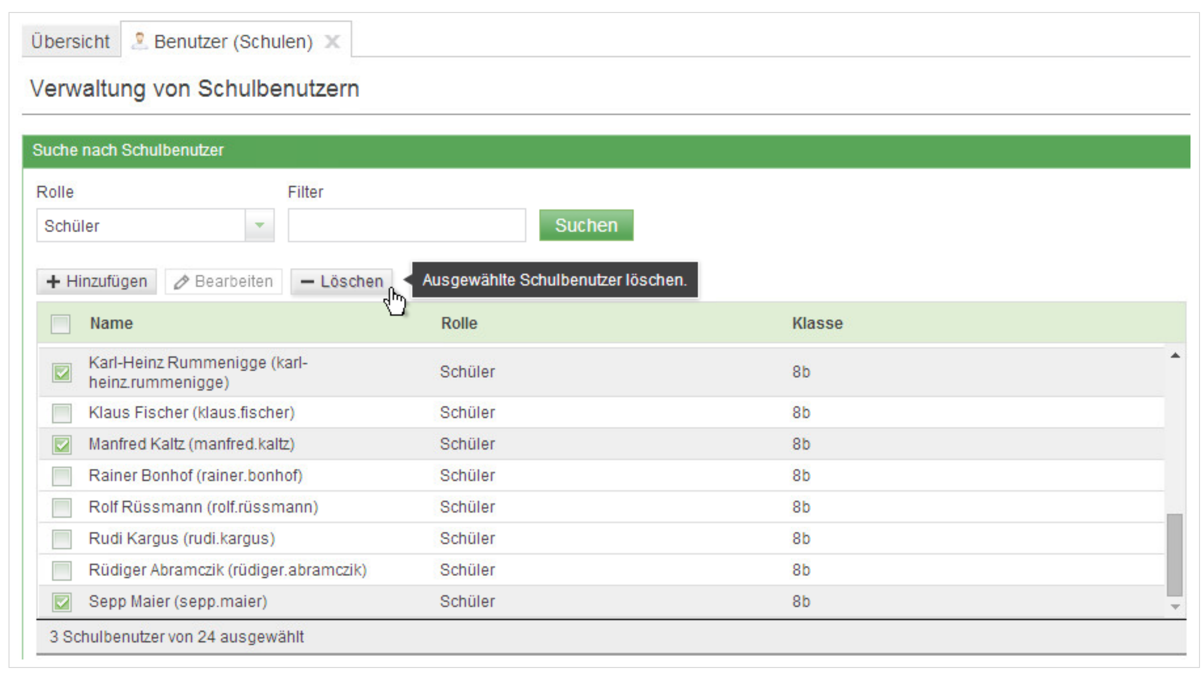


Abb. 49: Auswahl der zu löschenden Benutzer.

Eine letzte Bestätigung ist erforderlich, bevor die Daten gelöscht werden. Drücken Sie im nächsten Fenster nochmals auf „Löschen“, wenn die Schulbenutzer endgültig entfernt werden sollen

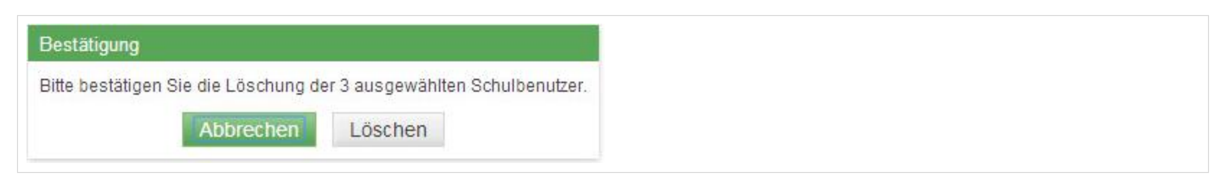


Abb. 50: Bestätigung des Löschvorganges.

3.5.1 Daten gelöschter Benutzer

Wenn ein Benutzer aus dem System gelöscht wird, wird der LDAP-Datensatz des Benutzers entfernt. Dadurch ist **mit sofortiger Wirkung**[12] keine Anmeldung am System möglich.

Die Daten des gelöschten Benutzers aus dessen Home-Verzeichnis werden nach */home/backup/BENUTZERNAME* gesichert. Dort kann ein administrativer Benutzer auf die Daten zugreifen, falls zum Beispiel der Benutzer versehentlich gelöscht wurde.

Alte Benutzerverzeichnisse aus */home/backup* müssen manuell gelöscht werden.

Daten, die ein Benutzer auf ein Tauschverzeichnis kopiert hat, werden nicht verschoben.

[12] Hier liegt ein Unterschied zur alten paedML Linux, in der es noch einen Zeitraum gab, in dem sich gelöschte Benutzer im Schulnetz anmelden konnten.

3.6 Änderung von Passwörtern

3.6.1 Änderung von Lehrer- und Schüler-Passwörtern

Aufruf über Schulkonsole: UCS@school Administration | Passwörter (Schüler)
Aufruf über Schulkonsole: UCS@school Administration | Passwörter (Lehrer)



Die Änderung von Passwörtern für Schüler und für Lehrer erfolgt nach dem gleichen Schema. Hier wird nur die Änderung von Schülerpasswörtern beschrieben.

Organisatorisch ist es vermutlich am einfachsten, wenn beim ersten IT-Unterricht durch den Lehrer ein Kennwort für alle Schüler der zu unterrichtenden Klasse gesetzt wird, das diese bei Ihrer ersten Anmeldung ändern müssen. Dieses Verfahren ist im Lehrerhandbuch beschrieben.

Für den Fall, dass Sie als Netzwerkberater Kennwörter (bspw. der Kollegen) ändern müssen, ist das Verfahren hier nochmals beschrieben.

Um Kennwörter zu ändern, navigieren Sie in der *Schulkonsole* in das Menü „*Schul-Administration* | *Passwörter (Schüler)*“.

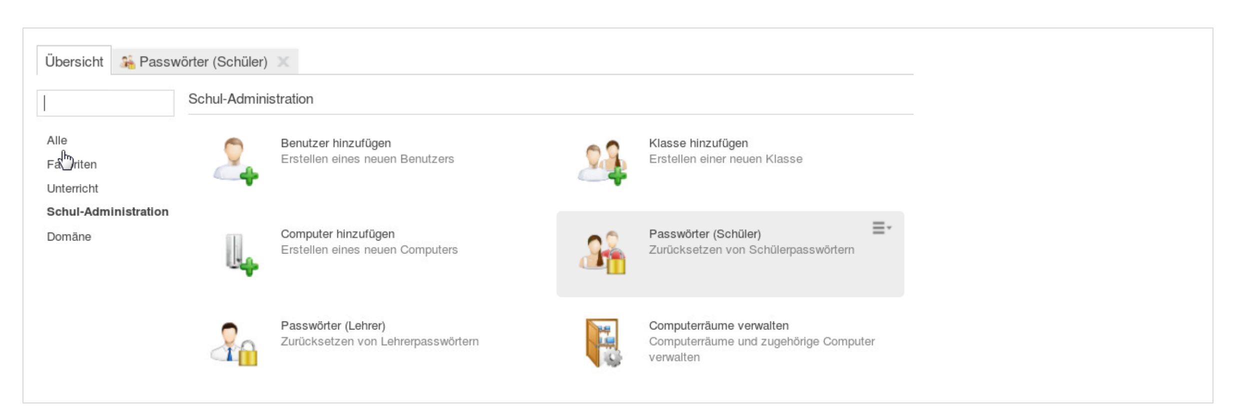


Abb. 51: Aufruf der Passwortänderung

Sie erhalten eine Übersicht über alle Schüler. Sie können über das Dropdownmenü „*Klasse oder Arbeitsgruppe*“ die Liste auf eine bestimmte Klasse verkleinern. Über das Suchfeld „*Name*“ und anschließenden Druck auf „*Suchen*“ können Sie einen Schüler direkt suchen. Sie können einzelne oder mehrere Schüler auswählen, deren Kennwort geändert werden soll. Markieren Sie hierfür die Checkboxen vor dem Namen der entsprechenden Schüler.

Drücken Sie auf „*Passwort zurücksetzen*“, um die Schülerkennwörter zu ändern.

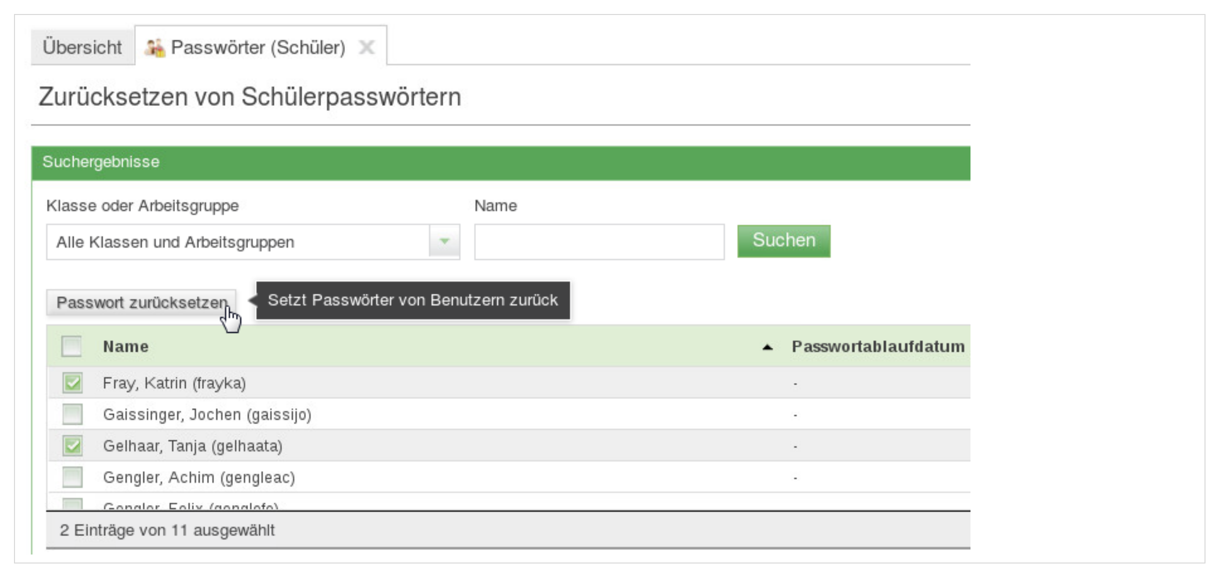


Abb. 52: Anzeige von Schülern für die Passwortänderung

In der folgenden Maske können Sie ein neues Kennwort eingeben. Dieses wird Ihnen zur Kontrolle im Klartext angezeigt. Sie können markieren, ob der Benutzer sein Passwort bei der nächsten Anmeldung ändern muss (empfohlen). Ein Klick auf „*Zurücksetzen*" ändert das Passwort.

Teilen Sie das neue Kennwort dem Benutzer mit.

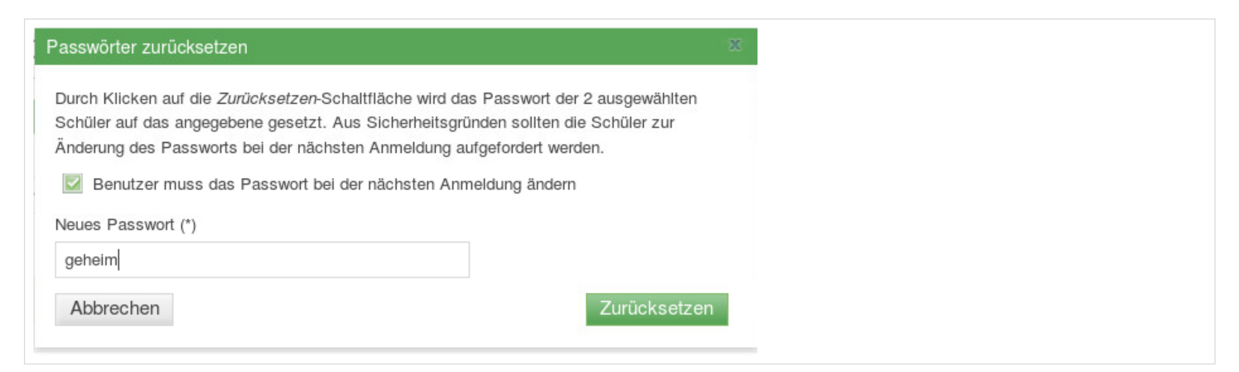


Abb. 53: Eingabe eines neuen Passworts

3.6.2 Änderung von Passwörtern administrativer Benutzer

Alle Passwörter von administrativen Benutzern werden bei der Installation des Systems mit dem Ausführen des Skriptes `lmz-initial-setup` auf denselben Wert gesetzt. Wird dieser Befehl nach der Ersteinrichtung erneut ausgeführt, werden im Hintergrund noch weitere Prozesse angestoßen. So wird beispielsweise das Server-Zertifikat neu generiert. Nach Möglichkeit sollten dieser Befehl also nicht ausgeführt werden. Stattdessen wird empfohlen die Kennwörter der administrativen Benutzer – wie im Folgenden beschrieben – zu ändern.

Die Kennwörter der Administratoren-Konten können wie folgt geändert werden:

Benutzer	Passwortänderung via
root	Passwortänderung an der Server-Konsole mit dem Befehl. Hierüber werden die Passwörter für den Benutzer „root" am Server und am Backupserver geändert: `#lmz-initial-setup --root`

Administrator	Änderung (**nur des Passwortes**) über das Schulkonsolenmenü „Domäne | Benutzer“.[13]
domadmin	Passwortänderung an der Server-Konsole mit dem Befehl `#lmz-initial-setup --domadmin`
netzwerkberater	Änderung (**nur des Passwortes**) über das Schulkonsolenmenü „Domäne | Benutzer“.[15]

Tabelle 8: Optionen für die Passwortänderung von administrativen Benutzern.

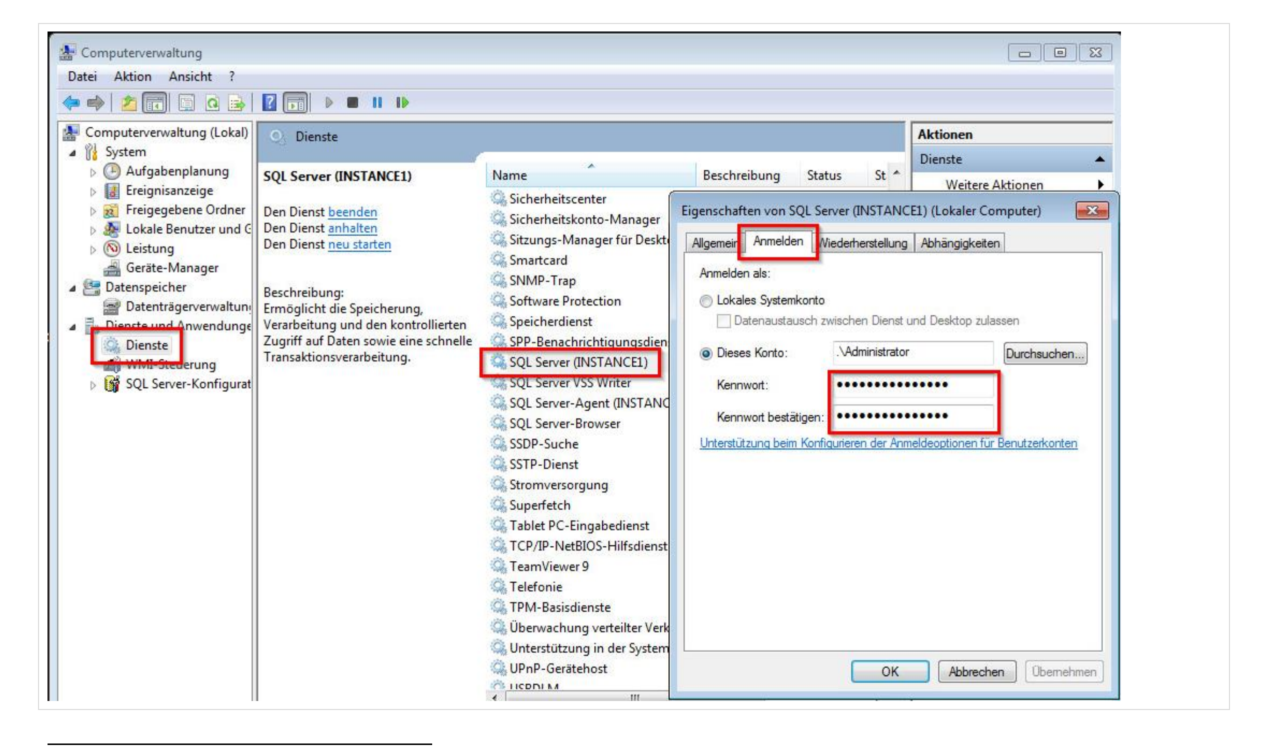
3.6.3 Optional: Änderung der Passwörter für SQL-Server



Dieser Abschnitt ist nur relevant, wenn Sie die *Windows*-Aktivierung über *VAMT* durchführen und das **Passwort des lokalen Administrators auf der** *AdminVM* (bzw. der Maschine, auf der *VAMT* installiert ist) geändert wird, nachdem die *opsi*-Produkte "*ms-vamt*" bzw. "*ms-sql-2012ee*" installiert wurden.

Näheres hierzu finden Sie in Kapitel 13.1 ab Seite 196.

Um das lokale Administratorkennwort auf dem SQL-Server zu hinterlegen, öffnen Sie die Computerverwaltung und navigieren dort auf „*Dienste* | *SQL Server (INSTANCE1)*“. Ein Doppelklick öffnet die Eigenschaften des SQL-Servers. Dort navigieren Sie in den Reiter „Anmelden“ und hier können Sie das neue Kennwort eintragen.



[13] Alternativ kann das Kennwort auch über Strg + Alt + Entf an einem Windows-Rechner geändert werden. Hierfür muss der entsprechende Benutzer natürlich an der Domäne angemeldet sein.

[15] Alternativ kann das Kennwort auch über Strg + Alt + Entf an einem Windows-Rechner geändert werden. Hierfür muss der entsprechende Benutzer natürlich an der Domäne angemeldet sein.

Abb. 54: Änderung des Administrator-Kennwortes für den SQL-Server

3.7 Passwort-Policy

3.7.1 Systemgenerierte Passwörter

Die Kennwörter, die die *paedML Linux* beim Benutzerimport anlegt, sind komplex. Sie bestehen aus **mindestens acht Zeichen** mit Groß- und Kleinbuchstaben, Zahlen und Sonderzeichen. Passwörter können nicht ausgelesen werden!

3.7.2 Von Benutzern angelegte Passwörter



Das System akzeptiert neue Kennwörter nur, wenn diese sich von den vorherigen Kennwörtern eines Benutzers unterscheiden. Hierbei werden die letzten drei Passwörter berücksichtigt, das heißt nach drei Passwortwechseln darf wieder ein altes Passwort verwendet werden.

Wenn ein Benutzer beispielsweise beim Login unter *Windows* nach der Änderungsaufforderung dasselbe Passwort verwendet, welches er bereits verwendet hatte, wird er bei jeder Anmeldung an der *Schulkonsole* erneut aufgefordert das Kennwort zu ändern. Erst durch das Setzen eines neuen Kennworts verschwindet die Änderungsaufforderung.

Die einzige Beschränkung bei benutzergenerierten Kennwörtern ist die Zeichenlänge von **mindestens acht Zeichen**.

3.8 Anlegen von Arbeitsgruppen

Aufruf über Schulkonsole: Schul-Administration | Arbeitsgruppen verwalten
Über Arbeitsgruppen können Sie *Projektarbeiten* innerhalb sowie außerhalb des regulären Klassenverbandes abbilden. So könnten Sie der Schulband, die sich aus verschiedenen Klassen zusammensetzt, in einem gleichnamigen Projekt Noten austeilen. Es ist aber auch möglich Projekte in Klassen anzulegen, um Arbeitsgruppen mit Material zu versorgen.

Eine genaue Beschreibung für den Umgang mit Arbeitsgruppen finden Sie im Lehrerhandbuch.

4. Verwaltung von Geräten



Bitte beachten Sie unbedingt die Hinweise zur Nomenklatur der *paedML Linux* im Anhang A, Seite 295.

Übersicht

- Zu Anfang dieses Kapitels stellen wir ein paar konzeptionelle Überlegungen an: Welche IP-Adressbereiche gibt es in der *paedML Linux?* Welche Systemrollen[16] können Clients erhalten? Wie ist die Systemrolle „*Windows*" definiert?
- In Kapitel 4.2 erfahren Sie, wie Rechner in die paedML Linux integriert werden können. Hierfür werden drei Verfahren – die Rechneraufnahme über eine Datei, die Rechneraufnahme via Netzwerk-Boot (PXE-Boot) und die Aufnahme über die Schulkonsole – beschrieben.
- Kapitel 4.3 behandelt die Netzwerkintegration von Geräten, die keine Computer sind. Hierzu zählen beispielsweise Netzwerkkomponenten oder Drucker.
- In Kapitel 4.4 gehen wir auf die Besonderheit von Geräten mit mehreren IP-Adressen (mobile Geräte mit WLAN- und Ethernet-Karte) ein.
- Das vierte Kapitel schließt mit dem Umbenennen und Löschen von Geräten aus dem pädagogischen Netz.

4.1 Vorbemerkungen

Die Domäne der *paedML Linux* arbeitet mit Namensauflösung (DNS). Alle Geräte im Netzwerk können über Ihren Netzwerknamen adressiert werden. Die Kenntnis von IP-Adressen ist für den Betrieb der paedML Linux daher nicht zwingend notwendig.

Beispiele zur Illustration:
Die Eingabe von https://server.paedml-linux.lokal in der Adressleiste Ihres Browsers führt Sie auf die Startseite des Servers.

Netzwerkbefehle wie bspw. `#ping` können ebenfalls auf einen DNS-Namen oder auf eine IP-Adresse ausgeführt werden. Um einen Rechner im Netzwerk zu pingen, kann dieser per Namen oder per IP-Adresse erreicht werden. Der DNS-Name eines Rechners (zum Beispiel r119-pc09) ist vermutlich einfacher zu merken als die IP-Adresse 10.1.0.153.

Bei der Aufnahme von neuen Geräten wird durch die Angabe von *10.1.0.0* (Netzadresse) die nächste freie IP-Adresse aus dem Adresspool der paedML (*10.1.0.32 bis 10.1.0.229*) vergeben. Sie brauchen sich also eigentlich keine Gedanken über IP-Adressen zu machen.

[16] Unter Systemrolle wird der Geräte-Typ in einem Univention-System verstanden. Hierbei handelt es sich um Betriebssysteme oder Geräte ohne Betriebssystem.

Allerdings ist ein strukturiertes Netzwerk mit fest vergebenen IP-Adressen durchaus sinnvoll, wenn Sie bspw. im IT-Unterricht mit IP-Adressen arbeiten wollen und hierfür wissen möchten, wie die Rechner in einem Raum zu erreichen sind. Sie können IP-Adressen bei der Rechneraufnahme auch selbst vergeben. Bitte wählen Sie hierfür jeweils eine Adresse zwischen *10.1.0.32* und *10.1.0.229*. Sollte die von Ihnen gewählte Adresse bereits vergeben sein, dann erhalten Sie eine Fehlermeldung.

Wir empfehlen Ihnen ausdrücklich, bei der manuellen Vergabe von IP-Adressen Ihr Netzwerk im Vorfeld der Installation zu planen und die IP-Adressierung entsprechend umzusetzen. Hinweise hierzu finden Sie im oben erwähnten Konzeptionsleitfaden[17].

Die folgende Tabelle gibt Ihnen eine Übersicht über den IP-Adressraum der *paedML Linux 6.0*.

[17] https://www.lmz-bw.de/technische-unterstuetzung/kundenportal/linux/dokumentationen.html

IP-Adressen	Was befindet sich im Adressraum?	Anzahl der verfügbaren IP-Adressen
10.1.0.0/24	Pädagogisches Netzwerk	254
10.1.0.1 - 10.1.0.20 10.1.0.1 10.1.0.2 10.1.0.5 10.1.0.10 10.1.0.11 10.1.0.12 10.1.0.13	Reservierte IP-Adressen Server Backup-Server („opsi-Server“) Webserver (optional) Router (optionales Gateway für das Routen in andere interne Netzwerke[18]) Firewall NAS zur Verwendung von BackupPC (optional) *AdminVM*	20
10.1.0.21 – 10.1.0.31	Frei verfügbarer Bereich für schuleigene Server	11
10.1.0.32 - 10.1.0.229	Arbeitsplatzrechner und Geräte im pädagogischen Netzwerk	198
10.1.0.230 - 10.1.0.254	DHCP-Pool für nicht registrierte Geräte, zum Beispiel bei der Rechneraufnahme	25
Weitere Netzsegmente der paedML Linux		
10.1.1.0/24	separates Lehrernetz	254
172.16.0.0/12 (172.16.0.0 – 172.31.255.255)	Adressbereich für Gäste-Netz (WLAN) – Anschluss über Firewall	1.048.576
192.168.255.0/24	Virtuelles Netz für OpenVPN – Anschluss über Firewall	254

Tabelle 9: IP-Adressen der paedML Linux.

4.1.1 Klärung der Systemrolle

Bei der Aufnahme eines neuen Rechners in die *paedML Linux* bekommt der Rechner einen Namen, eine IP-Adresse (optional: eine Inventarnummer) und eine Systemrolle, bzw. einen Systemtypen zugewiesen.

[18] Wird benötigt, falls die Schüle über VLAN mehrere Netzwerke abbilden will.

Bevor ein Gerät in die Domäne aufgenommen wird, sollte geklärt werden, um was für einen „Typ“ Gerät es sich handelt. Diese Zuordnung bestimmt, wie das Gerät von der paedML verwaltet wird. Bei der Aufnahme von Geräten in das Schulnetz stehen verschiedene Gerätetypen zur Auswahl:

Rechner-Typ Schulkonsole	Typ in CSV-Datei	Erklärung
Windows-System	*windows*	Client mit *Windows*
Univention Corporate Client	ucc	Clients mit Univention Linux (UCC)
Gerät mit IP-Adresse	ipmanagedclient	Drucker, Printserver, WLAN-Access-Points

Tabelle 10: Gerätetypen der paedML Linux

Bitte beachten Sie im Zusammenhang mit der Systemrolle die folgenden Hinweise:

- Der Typ „*Windows-System*“ wird für alle Clients verwendet, die Mitglied der paedML Domäne sind und mit *Microsoft Windows*-Betriebssystem betrieben werden. Dies ist unabhängig davon, ob die Rechner über Netzwerk gebootet und von opsi mit Software versorgt werden oder nicht.
- Der Typ „*Univention Corporate Client*“ ist nur für Clients, auf denen die Linux-Distribution *UCC* über PXE-Boot installiert werden soll[19].
- Bei Auswahl des Typs „*Gerät mit IP-Adresse*“ wird kein Computerkonto in der *Samba*-Domäne angelegt.
- Im Computerraummodul werden nur Clients des Typs „*Windows*-System“ und „Univention-Corporate-Client“ angezeigt.

4.1.2 Hinweise zur Systemrolle Windows-System

Windows-Rechner werden über den auf dem *Backup-Server* laufenden Dienst *opsi* verwaltet und von dort aus mit Betriebssystem, Software und Updates versorgt. Die Konfiguration läuft über den *opsi-config-editor* (siehe auch Kapitel 7, Seite 116).

Unterstützt werden die Betriebssysteme *Windows 7(64-Bit),* sowie *Windows 8.1 (64-Bit)*.

4.2 Aufnahme von Geräten in das paedML Netz



Achten Sie bei der Aufnahme der Rechner darauf, welche Firmware-Variante in den Rechnern verbaut ist. Das bisherige Firmware-System BIOS wird durch den Nachfolger UEFI[20] abgelöst, der in neuer Computerhardware verbaut ist.

opsi verwaltet Rechner mit den verschiedenen Firmware-Varianten unterschiedlich. Daher muss bei der Clientintegration darauf geachtet werden, um welches System es sich handelt.

Im Folgenden wird an den entsprechenden Stellen darauf hingewiesen, dass Sie

[19] Dieser Systemtyp wird aktuell für Thin-Clients genutzt, die in Modellschulen getestet werden.

[20] http://de.wikipedia.org/wiki/Unified_Extensible_Firmware_Interface

> darauf achten müssen, ob ein PC mit BIOS oder mit UEFI läuft.
>
> **Ein falsch angelegtes System kann nur durch Löschen und Neuaufnahme korrigiert werden.**

Um einen neuen Client in die *paedML Linux* aufzunehmen, können Sie drei Wege beschreiten:

1. Rechneraufnahme via PXE-Boot – Dieses Verfahren funktioniert nicht bei Rechnern mit UEFI, sondern nur mit BIOS. UEFI-Rechner müssen über eine der anderen Methoden in die Domäne aufgenommen werden.
2. Rechneraufnahme über eine Rechnerliste.
3. Rechneraufnahme über die *Schulkonsole.*

Die erste Möglichkeit Rechner aufzunehmen bedeutet einmalig „Turnschuhadministration“, d.h. Sie müssen jeden Rechner einzeln einschalten und registrieren.

Die anderen beiden Aufnahmeverfahren setzen voraus, dass Sie alle MAC-Adressen[21] der Netzwerkkarten kennen. Die Rechneraufnahme kann in diesen Fällen bequem von einem Schreibtischstuhl aus erledigt werden.

4.2.1 Aufnahme über Rechnerliste

Das zweite Verfahren ist sinnvoll, wenn Sie die gleichzeitige Aufnahme mehrerer Clients durchführen. Diese Aufnahme kann über eine Text-Datei erfolgen. Die Text-Datei für skriptbasierten Client-Import benötigt die folgenden Felder:

	Feld	Beschreibung	Beispiel
1	Rechner-Typ	Siehe Tabelle 10: Gerätetypen der paedML Linux“	*windows*
2	Hostname[22]	Name des Clients	pcraum2-pc12
3	MAC-Adresse	Wird für DHCP benötigt	00:0c:29:12:34:56
4	LDAP-OU	die LDAP-Schul-OU „schule“	schule[23]
5	IP-Adresse	IP-Adresse des Clients	10.1.0.0
6	Inventarnummer	optionale Inventarnummer	5146 Zimmer 114
7	In der paedML nicht belegt		
8	In der paedML nicht belegt		
9	In der paedML nicht belegt		
10	In der paedML nicht belegt		
11	BIOS/UEFI	0 = BIOS/ 1 = UEFI	1

---

[21] MAC-Adressen sind die eindeutigen IDs der Netzwerkkarten (vgl. http://de.wikipedia.org/wiki/MAC-Adresse)

[22] Bitte beachten Sie hierzu die Hinweise zur Nomenklatur in Anhang A

[23] Dieser Wert muss „schule“ heißen, da alle Objekte der paedML Linux im LDAP-Container „schule“ gespeichert werden!

12	Mehrere MAC-Adressen	kommagetrennte Liste von MAC-Adressen	00:0c:29:12:34:56, 00:0d:22:5c:d4:ac,

Tabelle 11: Felder der CSV-Datei für den skriptbasierten Client-Import

Hinweise:

Die ersten fünf Felder sind **Pflichtfelder**, um einen Rechner einzurichten. Jedes Rechnerobjekt muss in eine eigene Zeile geschrieben werden.

- Verwenden Sie als Trennzeichnen zwischen den Feldern einen *Tabulator*.
- Die Felder 7-10 sind derzeit nicht belegt. Fügen Sie entsprechend vier *Tabulatoren* ein.
- Der Hostname muss in der ganzen Schule eindeutig sein.
- Zulässige Zeichen sind Buchstaben ohne Umlaute, Ziffern sowie das Minuszeichen.
- Rechner mit mehreren MAC-Adressen können beim Import nur eine Adresse zugewiesen bekommen. Die Einrichtung mehrerer MAC-Adressen wird in Kapitel 4.4 ab Seite 80 beschrieben.
- Die *LDAP-OU* ist in der *paedML Linux* immer „*schule*“.
- Wird als IP-Adresse ein Subnetz angegeben (z.B. *10.1.0.0*), wird dem Client automatisch die nächste freie IP-Adresse aus diesem IP-Subnetz zugewiesen. Sie können hier aber auch eine feste IP-Adresse aus dem Adressbereich 10.1.0.32 - 10.1.0.229 vergeben.
- Die Netzmaske (im Feld „IP-Adresse“ einzugeben) kann sowohl als *Prefix* (*/24*) als auch in *Oktettschreibweise* (*255.255.255.0*) angegeben werden. Die Angabe der Netzmaske ist optional. Wird sie weggelassen, wird die Netzmaske *255.255.255.0* angenommen.

Die folgenden Felder (Feld sechs bis zwölf) sind optional, das bedeutet, dass der Import auch ohne diese Felder durchgeführt werden kann. Beachten Sie jedoch, dass die Reihenfolge eingehalten werden muss, falls Sie eines dieser Felder benutzen.

- Die *Inventar-Nummer* kann Buchstaben und Zahlen enthalten.
- Es folgen **vier leere Felder** (Trennzeichen = Tabulator).
- Im elften Feld wird der *Eintrag für UEFI oder BIOS* gesetzt. Der Wert *0* steht für ein herkömmliches *BIOS*, der Wert *1* steht für ein *UEFI*.

Beispiel einer Importdatei:

```
windows  pc01  d2:13:96:26:47:91  schule  10.1.0.0/24  →  →  →  →  →  →  1
windows  pc02  52:13:96:26:48:09  schule  10.1.0.0/24  →  →  →  →  →  →  0
```

Exportieren Sie die Rechner-Liste in eine Text-Datei. Nennen Sie die Datei „*rechner.txt*“.



Achten Sie beim Import von Listen (Benutzerlisten/Gerätelisten) auf die richtige Zeichencodierung[24] (Character Encoding) der Dateien.

Unterstützt wird nur der Zeichensatz ANSI. Bei anderen Zeichensätzen kann es zu Problemen beim Import von Daten kommen.

Die eben exportierte Datei „*rechner.txt*“ muss nun in das Home-Verzeichnis des Benutzers „*Administrator*“ kopiert werden, z.B. mit Hilfe von *WinSCP* oder dem *Windows-Explorer* (Vgl. Kapitel 1.4.3, Seite 33).



Das Kopieren der Datei auf den Server sollte von einem Rechner erfolgen, der im pädagogischen Netzwerk angeschlossen ist und per DHCP eine IP-Adresse bekommen hat. Außerdem sollten *WinSCP* (optional) und *PuTTY* auf dem Rechner installiert sein.

Öffnen Sie anschließend *PuTTY* (vgl. Kapitel 1.4.2 auf Seite 31) und loggen Sie sich mit den Zugangsdaten des Benutzers „root“ auf dem Server ein. Sie können sich auch direkt an einer Serverkonsole anmelden.

Navigieren Sie in das Verzeichnis, in das die Datei importiert wurde (`#cd /home/Administrator`). Führen Sie folgenden Befehl aus (ergänzen Sie dabei „*IMPORTDATEI.txt*“ durch den Namen Ihrer Datei):

```
#/usr/share/ucs-school-import/scripts/import_computer IMPORTDATEI.txt >>
/var/log/client_import.log 2>&1
```

Der Umbruch des Befehls ist darstellungsbedingt. Schreiben Sie den Befehl in eine Zeile!

Die importierten Rechnerobjekte werden nun so konfiguriert, dass jedes Mal, wenn sich ein Rechner an der Domäne anmeldet, dieser die angegebene IP-Adresse zugeordnet bekommt und der angegebene Hostname über das *Domain Name System* (DNS) aufgelöst werden kann.

[24] http://de.wikipedia.org/wiki/Zeichenkodierung

```
Processing of line 98 completed
20attach_pxe_boot_policy: Ignoring host g2r12-drucker (ipmanagedclient), no PXE boot policy availabl
e.
30add_to_ou_host_group: Ignoring host g2r12-drucker (type: ipmanagedclient), no host group available
.
Processing line 99: ipmanagedclient     nwt-drucker     00:0f:3c:ff:05:40       schule  10.1.0.205
verify ou for school nr schule already done
WARNING: no netmask specified for ip address 10.1.0.205 using 255.255.255.0
generate computer nwt-drucker (school schule)
verify ou for school nr schule already done
Network 10.1.0.0/24 exists in school schule!
set ip to 10.1.0.205 is not net 10.1.0.0
creating object cn=nwt-drucker,cn=computers,ou=schule,dc=paedml-linux,dc=lokal
Processing of line 99 completed
20attach_pxe_boot_policy: Ignoring host nwt-drucker (ipmanagedclient), no PXE boot policy available.
30add_to_ou_host_group: Ignoring host nwt-drucker (type: ipmanagedclient), no host group available.
Processing line 100: ipmanagedclient    kunst-drucker   00:0f:3c:ff:05:41       schule  10.1.0.206
verify ou for school nr schule already done
WARNING: no netmask specified for ip address 10.1.0.206 using 255.255.255.0
generate computer kunst-drucker (school schule)
verify ou for school nr schule already done
Network 10.1.0.0/24 exists in school schule!
set ip to 10.1.0.206 is not net 10.1.0.0
creating object cn=kunst-drucker,cn=computers,ou=schule,dc=paedml-linux,dc=lokal
Processing of line 100 completed
20attach_pxe_boot_policy: Ignoring host kunst-drucker (ipmanagedclient), no PXE boot policy availabl
e.
30add_to_ou_host_group: Ignoring host kunst-drucker (type: ipmanagedclient), no host group available
.
Processing line 101: ipmanagedclient    g1r315-drucker  00:0f:3c:ff:05:38       schule  10.1.0.203
verify ou for school nr schule already done
WARNING: no netmask specified for ip address 10.1.0.203 using 255.255.255.0
mac 00:0f:3c:ff:05:38 for computer g1r315-drucker already used (school schule)
Processing of line 101 completed
root@server:~# _
```

Abb. 55: Ausgabe an der Konsole nach Import von Geräten über eine Datei

4.2.2 Aufnahme via PXE-Boot



Das hier beschriebene Verfahren ist nur mit Rechnern durchführbar, die PXE-Boot unterstützen. Neue Rechner mit UEFI können derzeit noch nicht über PXE-Boot registriert werden und müssen an der Schulkonsole angelegt werden.

Um einen schuleigenen Rechner in Ihr Schulnetz aufzunehmen, schließen Sie diesen an das Netzwerk Pädagogik an (vgl. Grafik auf Seite 15).

Starten Sie den Rechner und stellen Sie im *BIOS* die Bootreihenfolge so ein, dass der Rechner zuerst über das Netzwerk (*PXE-Boot*), dann von der die Festplatte startet. Diese Einstellung sollte dauerhaft vorgenommen werden, damit spätere Änderungen[25] beim Hochfahren der Rechner angewandt werden können.

[25] Zum Beispiel Neuinstallation, Imagerestaurierung,… Diese Prozesse werden teilweise von *opsi* beim Systemstart initiiert.

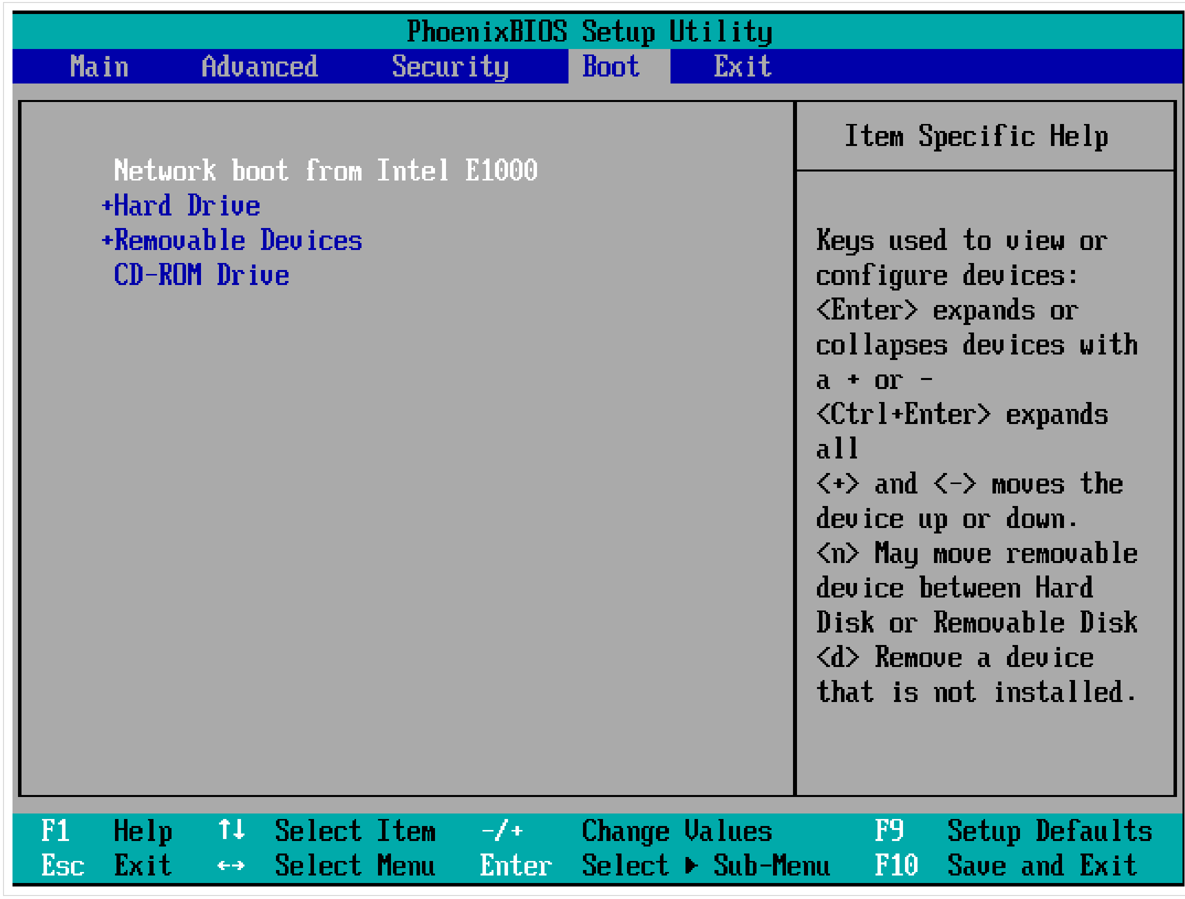


Abb. 56: Bootreihenfolge im Bios Menü. Starten Sie Schulclients immer über PXE-Boot

Speichern Sie die BIOS-Einstellung und starten Sie das Gerät neu.

```
Network boot from Intel E1000
Copyright (C) 2003-2008  VMware, Inc.
Copyright (C) 1997-2000  Intel Corporation

CLIENT MAC ADDR: 00 0C 29 B8 87 E3  GUID: 564DC319-235C-8B0C-508B-EAA5EAB887E3
CLIENT IP: 10.1.0.241  MASK: 255.255.255.0  DHCP IP: 10.1.0.1
GATEWAY IP: 10.1.0.11

PXELINUX 4.02 debian-20110423  Copyright (C) 1994-2010 H. Peter Anvin et al
!PXE entry point found (we hope) at 9E95:0106 via plan A
UNDI code segment at 9E95 len 0BDE
UNDI data segment at 98FF len 5960
Getting cached packet  01 02 03
My IP address seems to be 0A0100F1 10.1.0.241
ip=10.1.0.241:10.1.0.1:10.1.0.11:255.255.255.0
BOOTIF=01-00-0c-29-b8-87-e3
SYSUUID=564dc319-235c-8b0c-508b-eaa5eab887e3
TFTP prefix:
Trying to load: pxelinux.cfg/default                              ok
Loading ucc-1.0-lmz-desktop-image.img.kernel.._
```

Abb. 57: PXE-Boot – Der Computer lädt sich über das Netzwerk ein Betriebssystem

Beim Hochfahren sucht der Rechner nach bootbaren Images im Netzwerk. Der Server stellt ein *UCC*[26]-Linux-Abbild zur Verfügung, welches der Rechner startet. Über dieses Betriebssystem kann der Rechner in die Domäne aufgenommen werden.



Wenn der aufzunehmende Rechner nicht mit dem *UCC*-Linux-Abbild gestartet werden kann, empfehlen wir ausdrücklich die Rechneraufnahme über die Schulkonsole oder über die CSV-Datei vorzunehmen!

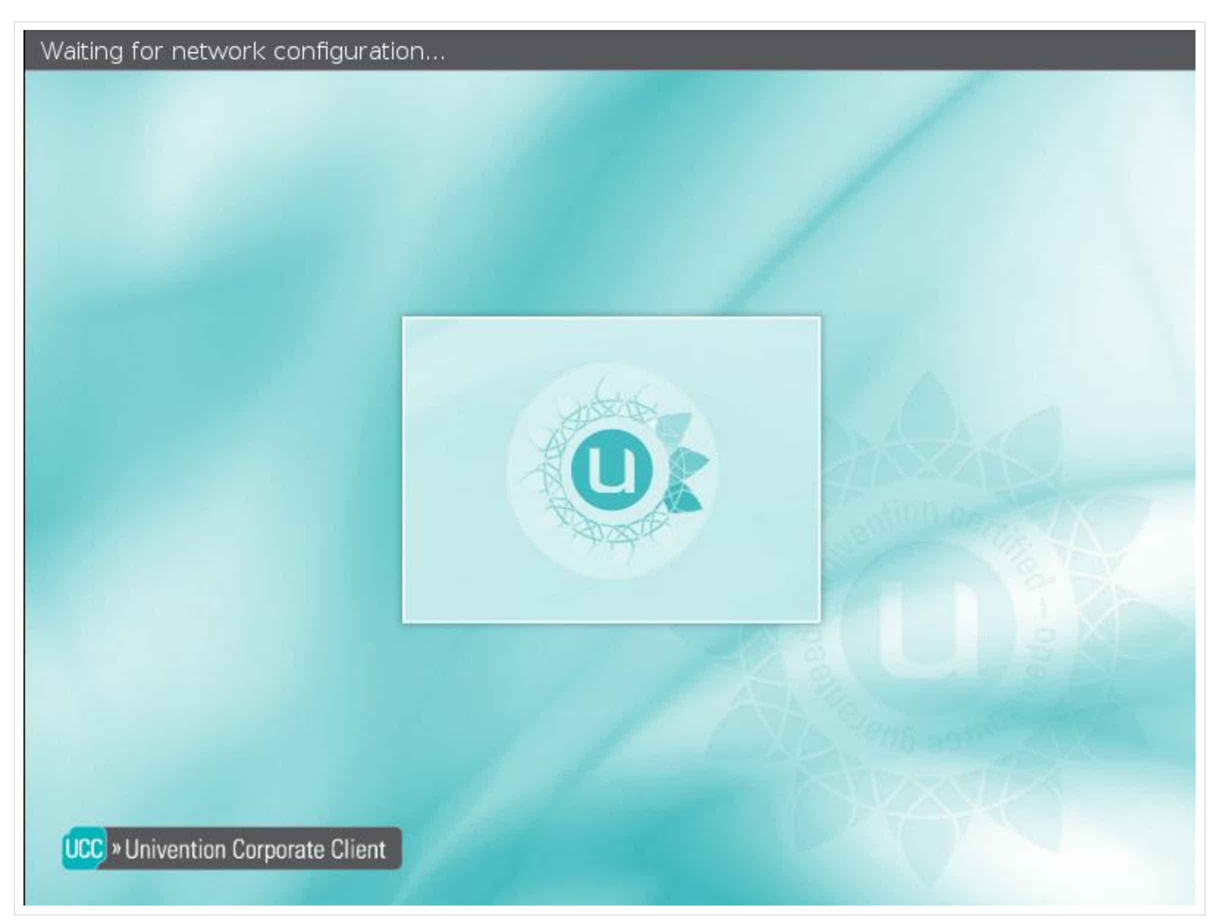


Abb. 58: Start des UCC-Live Systems für die Domänenaufnahme.

Die Konfiguration des *UCC*-Abbildes ist so eingestellt, dass automatisch ein Webbrowser (*Firefox*) mit *Schulkonsole* für die Domänenaufnahme des Clients geladen wird. Melden Sie sich hier zunächst als Benutzer „*domadmin*" an (das Kennwort entspricht – sofern nicht geändert – dem Administratorkennwort).

[26] UCC ist die Abkürzung von Univention Corporate Client

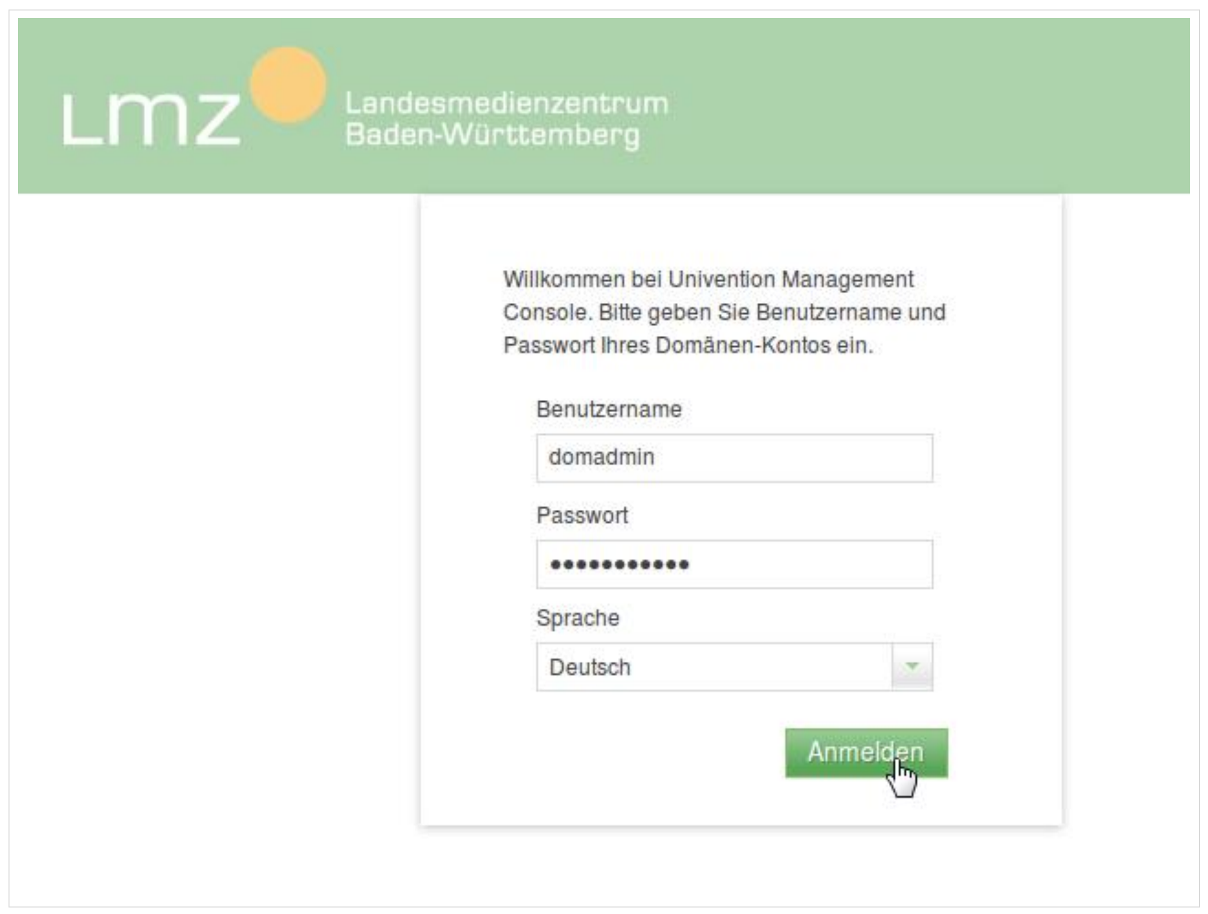


Abb. 59: Anmeldung an der Schulkonsole

Nach erfolgter Anmeldung können Sie zunächst bestimmen, was für ein Betriebssystem der Rechner später bekommen soll. Das Dropdown-Menü *Typ* gibt Ihnen hierfür verschiedene Auswahlmöglichkeiten (Vgl. Kapitel 4.1.1 ab Seite 66).

Wählen Sie „*Windows-System“*, wenn es sich um einen *Windows*-Rechner handeln soll.

Der Rechnertyp „*Univention Corporate Client*“ wird derzeit nicht verwendet.

Der Eintrag *Gerät mit IP-Adresse* ist für Netzwerkgeräte, z.B. Printserver oder WLAN-Accesspoints. Hierbei wird für das Gerät eine DHCP-Adresse reserviert und ein DNS-Eintrag erstellt. Es wird kein Computerkonto angelegt.



Wenn Rechner in das Schulnetz integriert, aber nicht über opsi verwaltet werden sollen, können Sie diese als „*Gerät mit IP-Adresse*“ in die Domäne aufnehmen.

Für Computer, die nicht der Schule gehören, empfehlen wir ausdrücklich KEINE Aufnahme in die Schuldomäne, sondern eine Integration in das Gäste-Netzwerk.

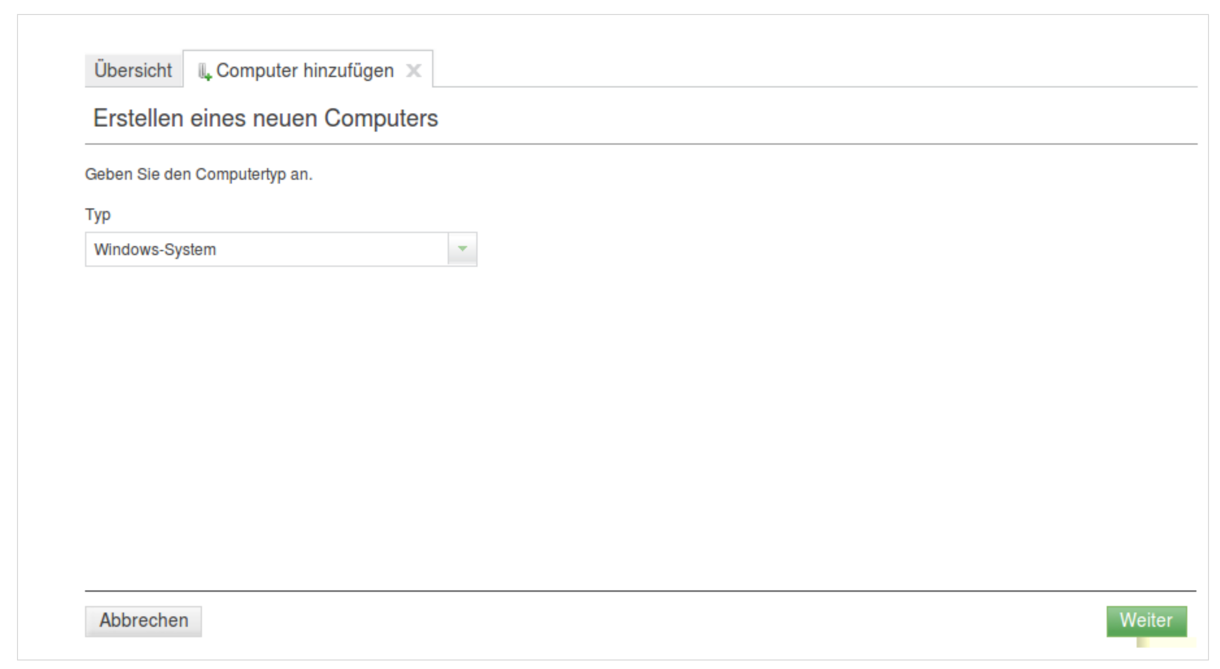


Abb. 60: Eingabe für Computertyp

Die folgende Maske hilft Ihnen dabei, den Rechner für die Domäne zu konfigurieren. Geben Sie hierfür den „*Namen*“[27] und die „*IP-Adresse*“ des Rechners ein. Die Eingabe der Netz-Adresse „*10.1.0.0*“ vergibt die nächste freie IP-Adresse im Adresspool. Wenn Sie eine eigene Adresse vergeben wollen, dann wählen Sie bitte eine Adresse zwischen „*10.1.0.32*“ und „*10.1.0.229*“.

Der Wert der Subnetzmaske ist vorgeschrieben und darf nicht geändert werden.

Die „*MAC-Adresse*“ der Netzwerkkarte, mit der die Verbindung zum Server aufgebaut wurde, wird automatisch angezeigt.

Falls Ihre Hardware inventarisiert ist, können Sie die „*Inventarnummer*“ angeben.



Bei der Rechneraufnahme über den PXE-Boot darf der Haken bei „*UEFI*“ nur dann gesetzt werden, wenn das Gerät nach der Aufnahme auf UEFI-Modus gestellt werden kann.

Der Haken darf nur bei Geräten des Typs „*Windows-System*“ gesetzt werden.

Speichern Sie die Werte, um Änderungen zu übernehmen. Falls das System Fehler entdeckt (doppelte Namen, MAC- oder IP-Adressen) bekommen Sie eine Meldung mit der Aufforderung, den Datensatz zu korrigieren.

[27] Bitte achten Sie unbedingt darauf, Namen für Objekte in der Schule eindeutig zu vergeben.

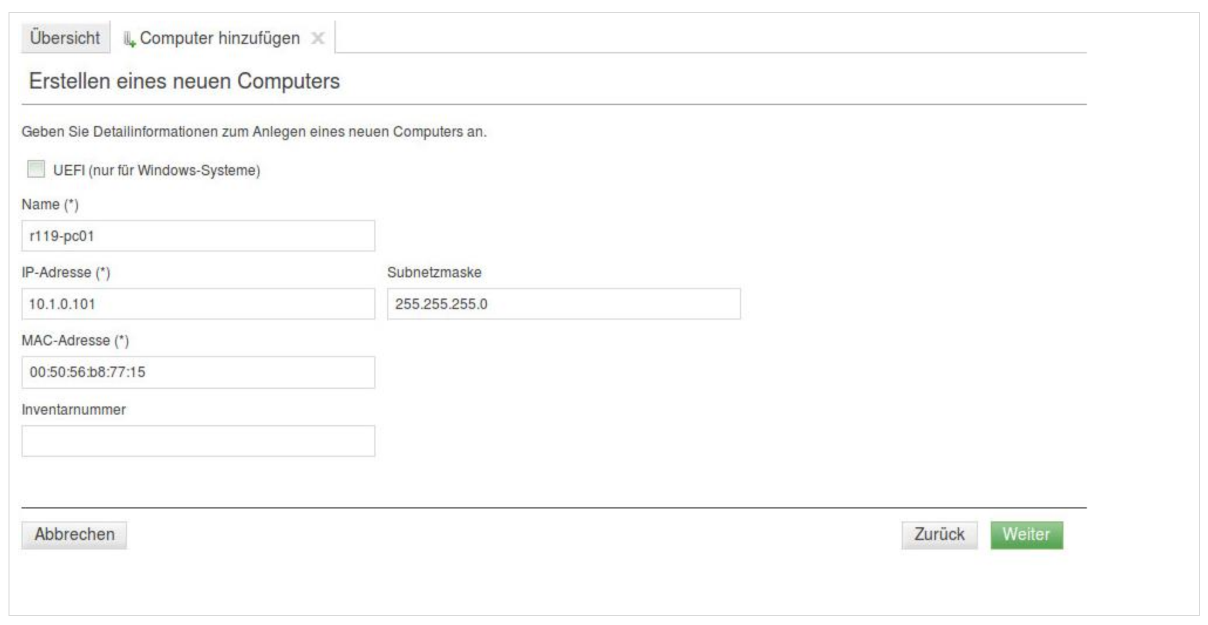


Abb. 61: Rechneraufnahme

Das System quittiert die Neuaufnahme mit einer Meldung am oberen Bildschirmrand. Diese Meldung wird nur kurz eingeblendet. Bis zum Erscheinen dieser Anzeige kann es unter Umständen bis zu einer Minute dauern. Bitte warten Sie darauf, dass die Anzeige erscheint, bevor Sie fortfahren.

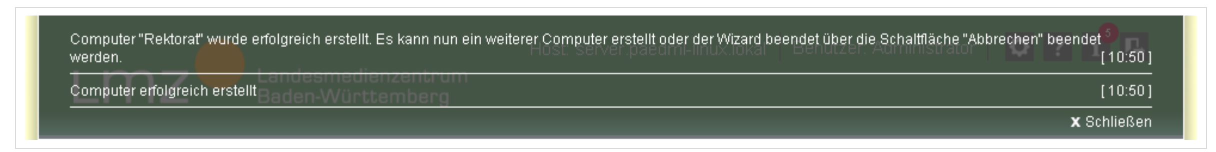


Abb. 62: Computer wurde erfolgreich erstellt.

Nun können Sie den Computer herunterfahren, indem Sie sich an der Schulkonsole abmelden.

Sie haben hierfür zwei Möglichkeiten:

1. Schalten Sie den Rechner einfach aus

   oder

2. Fahren Sie den Rechner kontrolliert herunter

Schließen Sie zunächst das Browserfenster durch Drücken auf das verborgene X, das eingeblendet wird, wenn Sie den Mauszeiger auf den oberen Bildschirmrand bewegen.



Abb. 63: Schließen des Browserfensters

Der UCC-Client startet anschließend eine Linux-Anmeldemaske, aus der Sie den Rechner ausschalten können. Drücken Sie hierfür auf das Computersymbol oben links und dort auf „*Shut Down*“. Im nächsten Dialog müssen Sie das Herunterfahren nochmals mit einem Klick auf „*Shut Down*“ bestätigen.

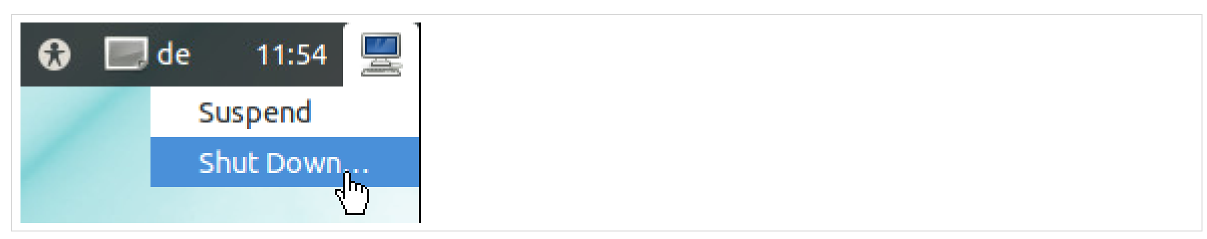


Abb. 64: Rechner herunterfahren

4.2.3 Rechneraufnahme über die Schulkonsole

Aufruf über Schulkonsole: Schul-Administration | Rechner (Schulen)
Eine weitere Möglichkeit Rechner in das Netzwerk zu integrieren bietet die *Schulkonsole*. Bitte beachten Sie, dass Sie für diesen Weg alle MAC-Adressen der aufzunehmenden Rechner kennen müssen.

Melden Sie sich als *Administrator* an der *Schulkonsole* an und öffnen Sie das Menü „*Schul-Administration*". Hier wählen Sie den Menüpunkt „*Rechner (Schulen)*".

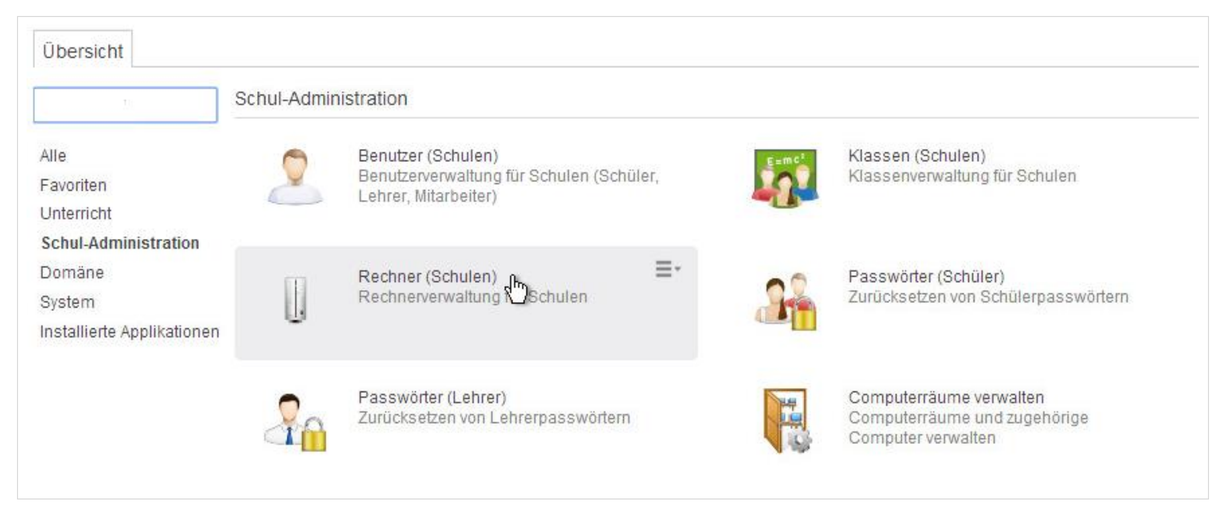


Abb. 65: Neuanlegen von Rechnern über Menüpunkt Rechner Schulen

Es öffnet sich eine neue Maske mit der Übersicht über alle im System angelegten Geräte. Klicken Sie oben links auf den Knopf „*Hinzufügen*", um ein neues Rechnerobjekt zu erstellen.

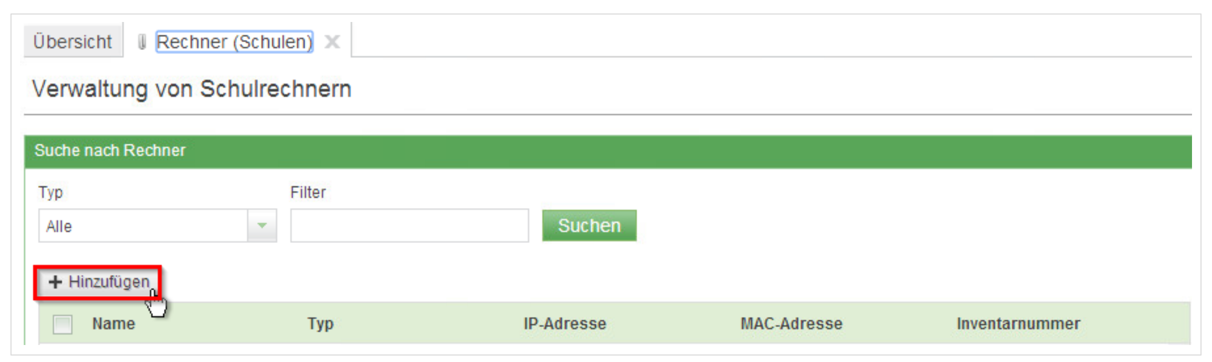


Abb. 66:

In der nächsten Maske können Sie bestimmen, was für ein Betriebssystem der Rechner später bekommen soll. Das Dropdown-Menü „*Typ*" gibt Ihnen hierfür verschiedene Auswahlmöglichkeiten.

Wählen Sie *„Windows-System“*, wenn es sich um einen *Windows*-Rechner handeln soll.

Der Rechnertyp „*Univention Corporate Client*“ wird derzeit in der *paedML Linux* nicht verwendet.

Der Rechnertyp „*Mac OS X*“ wird derzeit in der *paedML Linux* nicht verwendet.

Der Eintrag *Gerät mit IP-Adresse* ist für Netzwerkgeräte, z.B. Printserver bzw. WLAN-Accesspoints vorgesehen. Hierbei wird für das Gerät eine DHCP-Adresse reserviert und ein DNS-Eintrag erstellt. Es wird kein Computerkonto angelegt.

Bestätigen Sie Ihre Auswahl mit „*Weiter*“.

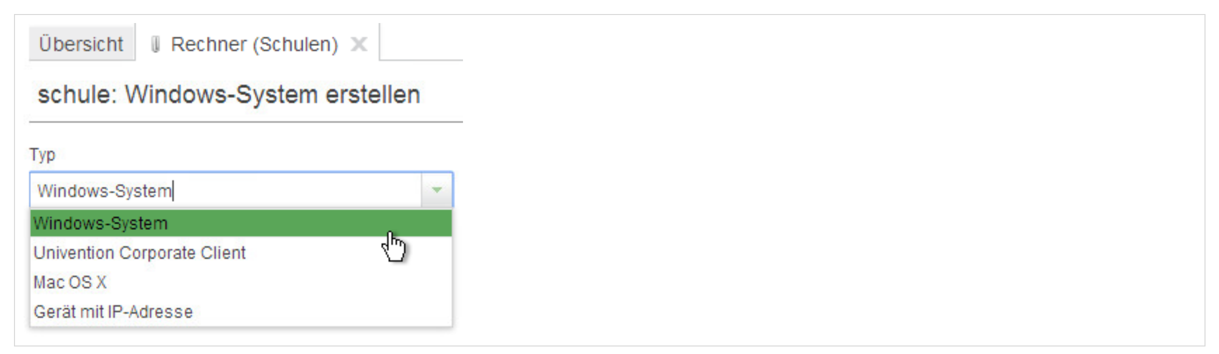


Abb. 67: Was für ein Client soll in das Schulnetzwerk integriert werden?

Die folgende Maske hilft Ihnen dabei, den Rechner für die Domäne zu konfigurieren. Geben Sie hierfür den „*Namen*[28]“ und die „*IP-Adresse*“ des Rechners ein. Die Eingabe der Netz-Adresse „*10.1.0.0*“ vergibt die nächste freie IP-Adresse im Adresspool. Wenn Sie eine eigene Adresse vergeben wollen, dann wählen Sie bitte eine Adresse zwischen *10.1.0.32* und *10.1.0.229*.

Wenn es sich um ein Gerät mit UEFI-Firmware handelt, muss zusätzlich der Haken bei „*UEFI*“ gesetzt werden. Setzen Sie diesen Haken **NUR** bei Geräten des Typs „*Windows-System*“!

Der Wert der „*Subnetzmaske*“ ist vorgeschrieben und darf nicht geändert werden.

Die „*MAC-Adresse*“ des aufzunehmenden Rechners muss in das entsprechende Feld eingetragen werden. Bitte beachten Sie für die Einrichtung eines Computers mit mehreren Netzwerkkarten den Hinweis am Ende dieses Unterkapitels.

Falls Ihre Hardware inventarisiert ist, können Sie die „*Inventarnummer*“ angeben.

Speichern Sie die Werte mit „*Weiter*“, um Änderungen zu übernehmen. Falls das System Fehler entdeckt (doppelte Namen, MAC- oder IP-Adressen, nicht zulässige Sonderzeichen) bekommen Sie eine Meldung mit der Aufforderung, den Datensatz zu korrigieren.

[28] Bitte achten Sie unbedingt darauf, Namen für Objekte in der Schule eindeutig zu vergeben.

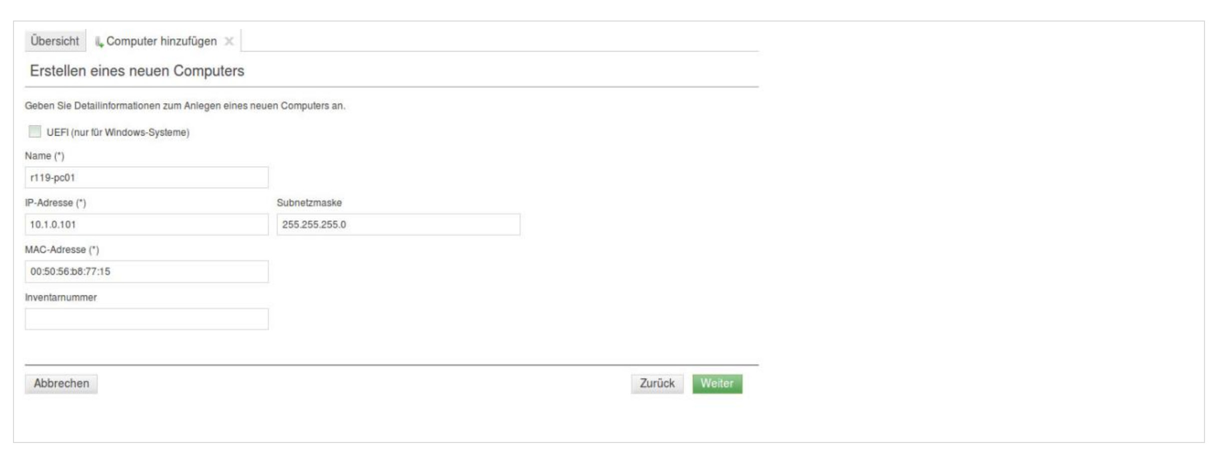


Abb. 68: Rechneraufnahme

Das System quittiert die Neuaufnahme mit einem Hinweis, der nur kurz eingeblendet wird.

Wenn Sie wollen, können Sie anschließend weitere Rechner aufnehmen oder das Untermenü verlassen.

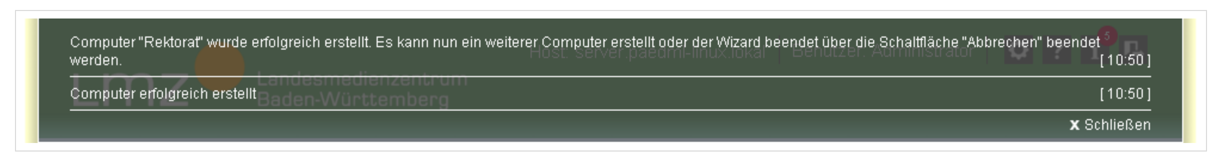


Abb. 69: Computer wurde erfolgreich erstellt.

4.3 Integration von Netzwerkkomponenten

Die bisher beschriebenen Verfahren gelten für Rechner, die von der *paedML* verwaltet werden sollen. Diese Rechner werden in der Regel über *opsi* installiert und bekommen Softwarepakte über *opsi* verteilt. Es gibt jedoch Geräte, die nicht in diese Kategorie fallen.

Hierzu zählen zum Beispiel:

- Netzwerkgeräte (wie Router, Switches, Accesspoints) mit eigener IP-Adresse
- Drucker mit Netzwerkanschluss
- Computer, die in das Netzwerk aufgenommen, aber nicht via opsi verwaltet werden sollen[29].

Diese Geräte werden wie oben beschrieben in das Netzwerk eingebunden, es wird jedoch bei der Auswahl des *Computeryps* der Wert *„Gerät mit IP-Adresse“* ausgewählt. Bei Verwendung dieses Typs wird nur eine DHCP-Reservierung angelegt und kein Computerkonto in der Domäne.

[29] Zum Beispiel Rechner, die mit OEM-Lizenzen beschafft wurden oder Maschinen, die von Kollegen betreut werden, die nicht als Netzwerkberater agieren. Wir möchten in diesem Zusammenhang darauf hinweisen, dass private Rechner jedweder Art nichts im Schulnetz zu suchen haben. Deren Einbindung sollte über das Gäste-Netz geschehen.



Für Computer, die nicht der Schule gehören, empfehlen wir ausdrücklich eine Anbindung über das Gäste-Netz.

4.4 Geräte mit mehreren Netzwerkkarten

Aufruf über Schulkonsole (als Administrator): Domäne | Rechner
Die Aufnahme von Clients mit mehreren Netzwerkkarten über eine Import-Datei ist in Kapitel 4.2.1 auf Seite 68 beschrieben. In diesem Abschnitt wird beschrieben, wie an Rechner, die bisher nur mit einer Netzwerkkarte im System geführt werden, weitere Netzwerkkarten zugewiesen werden.

Hierfür müssen Sie nach dem Anlegen des Rechners in die *Schulkonsole* wechseln und das Rechnerobjekt bearbeiten. Sie können jedem Gerät weitere MAC-Adressen zuweisen.



Pro Rechner darf es nur eine IP-Adresse geben.

Es können in einem Rechnerobjekt mehrere Netzwerkkarten hinterlegt werden. So kann beispielsweise ein Laptop mit Kabelverbindung und mit WLAN-Karte im Netz betrieben werden. Der Rechner bekommt vom Server immer die gleiche IP –Adresse bei der Anmeldung am Netzwerk.



Die hier beschriebenen Einstellungen haben den Vorteil, dass die Rechner immer mit derselben IP-Adresse (Kabel oder WLAN) an das Netzwerk angeschlossen sind.

Wichtig: Die Beschränkung auf eine IP-Adresse ist notwendig, da sowohl das Computerraum-Modul der SK sowie opsi nur mit einer IP-Adresse pro Client umgehen können!

Hinweis: Der gleichzeitige Anschluss beider NICs sollte vermieden werden, da nur eine Karte die richtige IP-Adresse bekommt.

Im Menüpunkt „*Domäne* | *Rechner*“ finden Sie eine Liste aller Clients des Schulnetzes. Wählen Sie sich das Gerät, dem Sie eine zweite Netzwerkkarte zuweisen wollen und öffnen Sie dieses mit einem Mausklick.

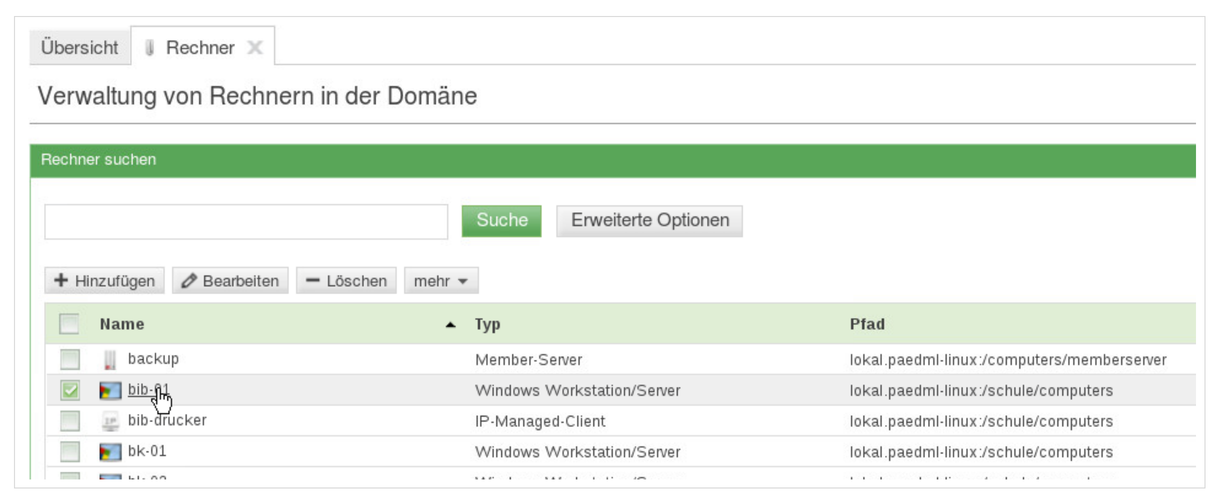


Abb. 70: Auswahl des zu bearbeitenden Gerätes

Scrollen Sie in dem sich öffnenden Fenster bis zu den „*Netzwerk-Einstellungen*“. Drücken Sie auf das *+-Symbol* und tragen Sie in das entsprechende Feld unter der vorhandenen „*MAC-Adresse*“ die MAC-Adresse der zweiten Netzwerkkarte ein.

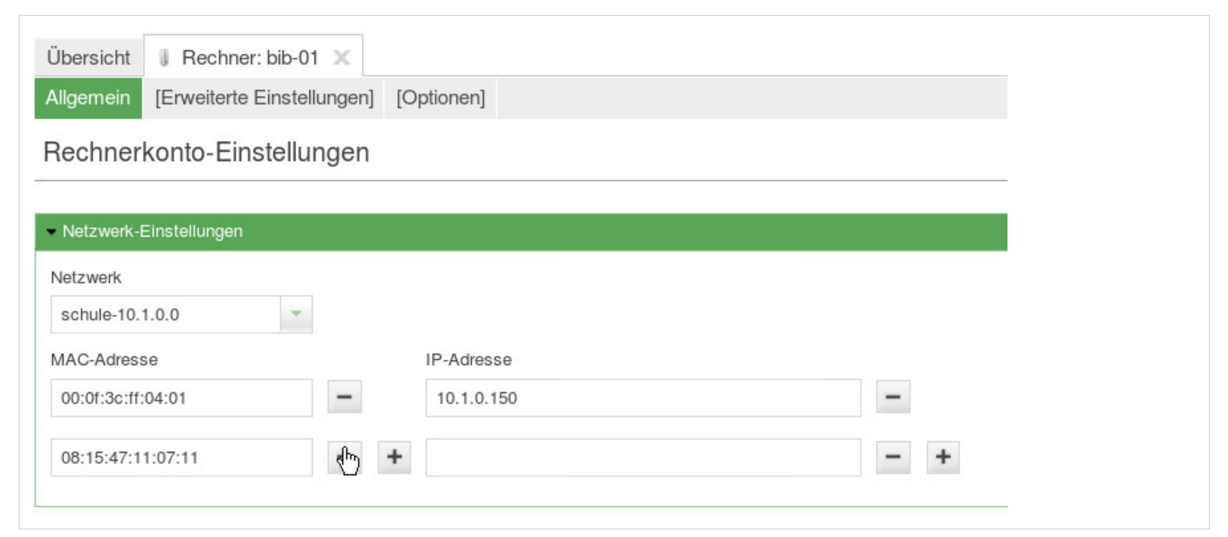


Abb. 71: Eintragen einer weiteren MAC-Adresse

Scrollen Sie noch weiter nach unten bis zu dem Feld „*DHCP*“. Dort befinden sich drei Dropdownmenüs, die wie folgt befüllt werden müssen:

Feld	Wert
DHCP-Dienst	schule
IP-Adresse	Dieselbe Adresse, die der Rechner schon für die andere Netzwerk-Karte zugewiesen bekommen hat.
MAC-Adresse	Die oben eingegebene MAC-Adresse der zweiten Netzwerkkarte

Tabelle 12: Einträge im Feld DHCP

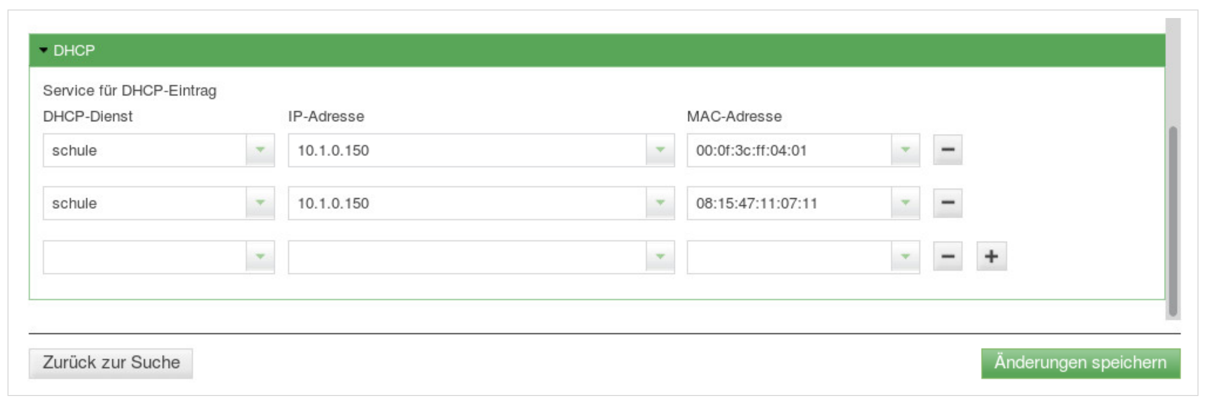


Abb. 72: Einstellungen für den DHCP-Server

Übernehmen Sie die Änderungen mit „*Änderungen speichern*“.



Mögliche Probleme mit Tablets:

Da Tablets in der Regel nicht über Netzwerkkarten verfügen, gibt es häufig die Möglichkeit mit USB-Ethernet-Adaptern eine Kabelverbindung zum Netzwerk herzustellen. Über diese Kabelverbindung kann ein Gerät beispielsweise mit neuer Software versorgt werden. Jeder dieser USB-Ethernet-Adapter hat eine eigene MAC-Adresse.

ACHTUNG! Da diese USB-Geräte mobil sind, könnte der USB-Ethernet-Adapter zu einem anderen Tablet wandern und die Client-Registrierung, welche an die MAC-Adresse gebunden ist, würde fälschlicherweise mitwandern. Folgende Fehler könnten hierbei auftreten:

- Geräte erhalten evtl. die falsche IP-Adresse – erstmal nicht schlimm
- Im Computerraum werden die Geräte im falschen Raum angezeigt, bzw. es wird das falsche Tablet als online angezeigt – störend.
- Beim Rollout wird das falsche Gerät ausgerollt, bzw. nichts ausgerollt – problematisch.

Im Falle eines Rollouts muss der Administrator sicherstellen, dass das richtige Gerät mit dem richtigen Adapter ausgerollt wird.

Daher empfehlen wir pro Tablet einen eigenen Adapter zu beschaffen. Alle Adapter sollten mit der MAC-Adresse beschriftet und (per Markierung) einem Gerät zugewiesen werden. Jedes Tablet sollte ausschließlich mit dem ihm zugewiesenen Adapter betrieben werden.

4.5 Ändern und Löschen von Geräten

4.5.1 Neuer Name bestehender Geräte

Aufruf über Schulkonsole (als Administrator): Domäne | Rechner



Da das Umbenennen von Geräten über die Schulkonsole nicht möglich ist, müssen Sie Geräte löschen und neu anlegen, wenn deren Name geändert werden soll.

Dieser Löschvorgang wird im folgenden Abschnitt beschrieben.

Anschließend müssen alle neu angelegten Rechner erneut mit opsi eingerichtet werden (Betriebssystem und Software).

Die Verwaltung der Rechner geschieht über das Schulkonsolenmodul „*Domäne* | *Rechner*“, das Sie als *Administrator* aufrufen müssen.

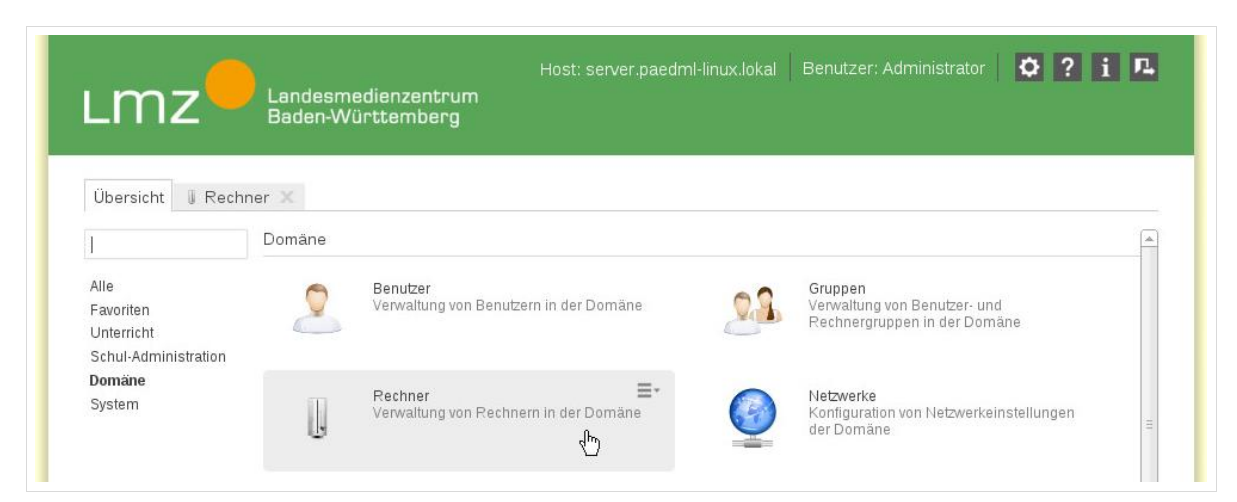


Abb. 73: Aufruf der Rechnerverwaltung

Nach Aufruf des „*Rechner*“-Moduls bekommen Sie eine Liste aller im System angelegten Geräte angezeigt. Hier werden nicht nur Rechner, sondern alle Geräte, also auch Drucker und andere „*Geräte mit IP-Adresse*“ angezeigt.

Um einen Eintrag zu löschen, markieren Sie die Checkbox vor dem Gerät. Oberhalb der Liste werden jetzt Schaltflächen angezeigt. Klicken Sie auf die Schaltfläche „*Löschen*“, um den Eintrag aus dem System zu entfernen.



Bitte beachten Sie, dass in dieser Liste ALLE Geräte der paedML Linux angezeigt werden und ein unbedachtes Löschen (zum Beispiel das Entfernen des Servers) unangenehme Folgen haben kann.

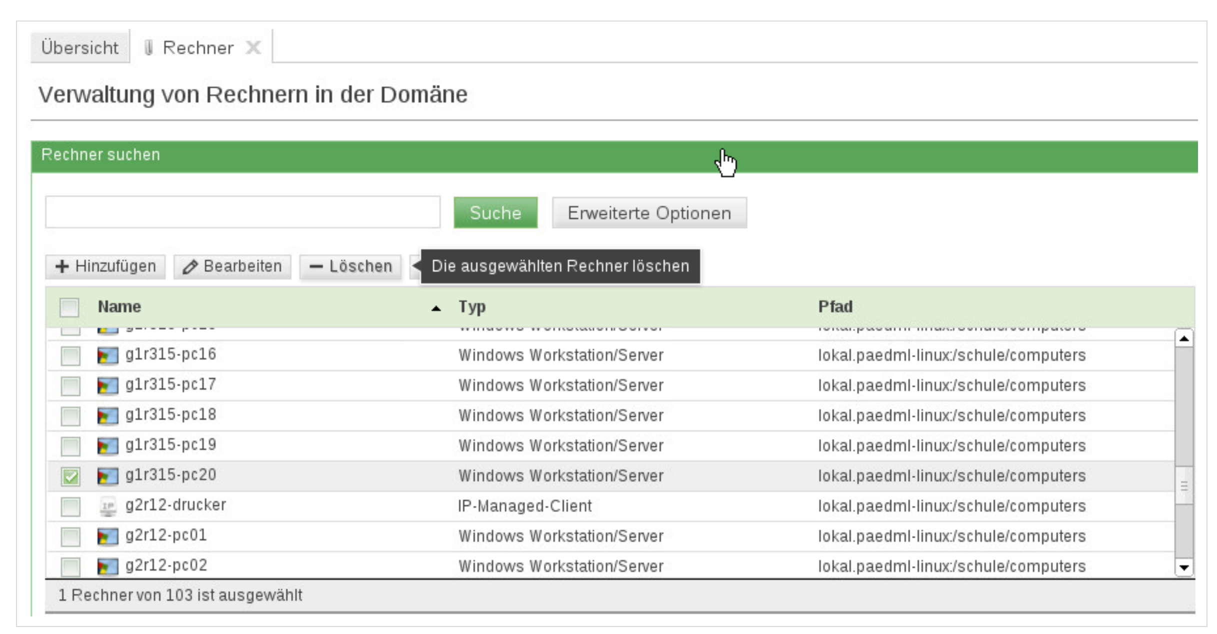


Abb. 74: Ein Rechner wurde zum Löschen markiert.

Bevor das Gerät aus dem System gelöscht werden kann, müssen Sie in einem Dialogfenster den Löschvorgang bestätigen. Achten Sie dabei darauf, dass der Haken bei „*Zugehörige Objekte löschen*“ gesetzt ist.

4.5.2 Änderung der IP-Adresse bestehender Geräte

Aufruf über Schulkonsole (als Administrator): Domäne | Rechner



Bei der nachträglichen Änderung von IP-Adressen über die *Schulkonsole* ist zu beachten, dass Geräte vom Rechner-Typ „*Windows-System*“ Anpassungen benötigen, ohne die die Änderung der IP-Adresse zu unerwünschtem Verhalten führt[30].

Die nachträgliche Änderung der IP-Adresse geschieht als *Administrator* im Schulkonsolenmodul „*Domäne | Rechner*“.

Rufen Sie das *Schulkonsolen*-Menü auf und wählen Sie den Rechner, der bearbeitet werden soll.

[30] Konkret würde ein Rechner mit geänderter IP-Adresse nicht – wie gewünscht – über Netzwerk in *opsi* bzw. *Windows* starten. Stattdessen würde die Aufnahmemaske für neu anzulegende Clients erscheinen.

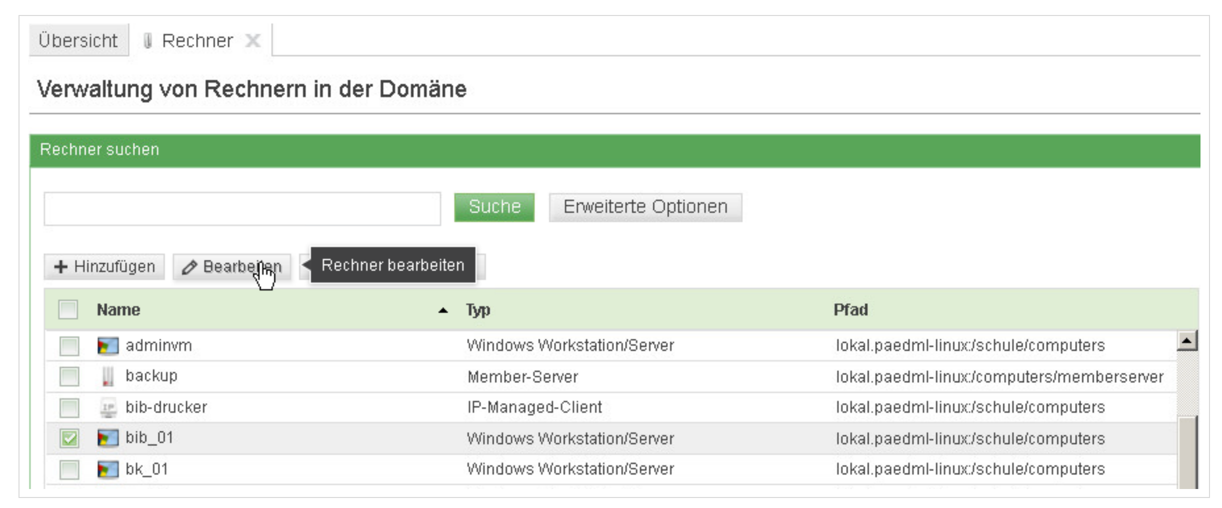


Abb. 75: Der Rechner bib_01 soll eine neue IP-Adresse bekommen.

Im Reiter „*Allgemein*“ im Abschnitt „*Netzwerk-Einstellungen*“ tragen Sie die neue IP-Adresse ein (roter Kasten). Die neue IP-Adresse muss in dieser Maske mehrfach eingetragen werden. Ein rotes Ausrufezeichen markiert die Felder, in denen die Änderung vorgenommen werden muss. Scrollen Sie die Maske nach unten und ändern Sie jedes Feld mit rotem Ausrufezeichen (vgl. roter Kreis) in den Wert der neuen IP-Adresse.

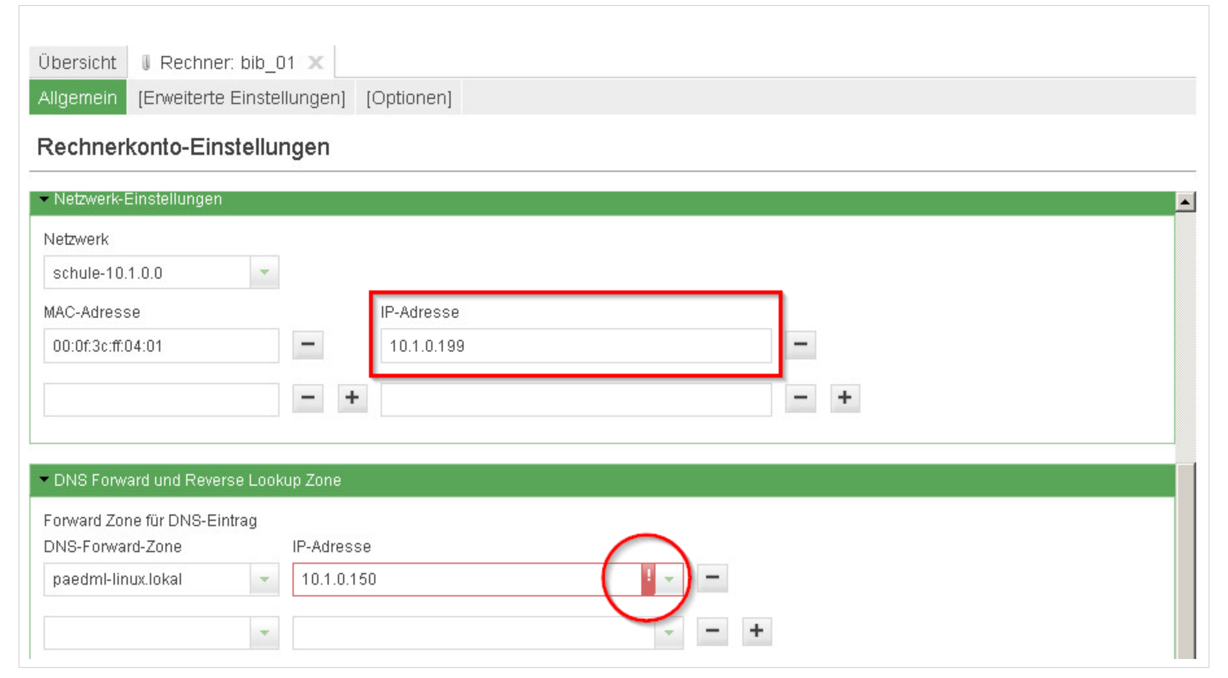


Abb. 76: Die neue IP-Adresse muss mehrfach eingegeben werden.

Wenn nicht alle notwendigen Felder geändert wurden, erscheint ein Warnhinweis.

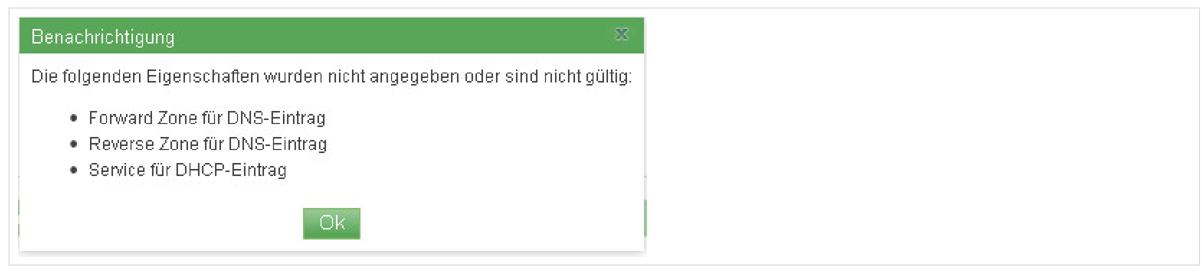


Abb. 77: Warnhinweis bei unvollständiger Änderung der Maske.

Übernehmen Sie die Änderungen an dem Rechnerobjekt mit „*Änderungen speichern*".

Anschließend öffnen Sie das Schulkonsolenmenü „*Domäne | DHCP*".

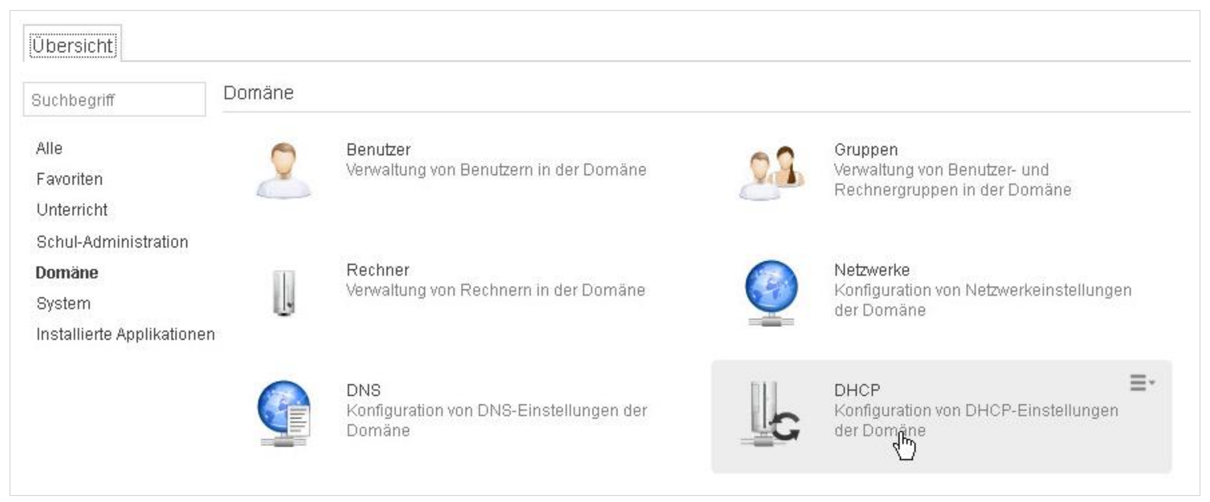


Abb. 78: Öffnen von Domäne | DHCP

In der sich öffnenden Maske „*Konfiguration von DHCP-Einstellungen der Domäne*" wählen Sie den soeben geänderten Rechner aus. Dieser sollte im Container „*schule*" liegen. Öffnen Sie das Bearbeitungsmenü.

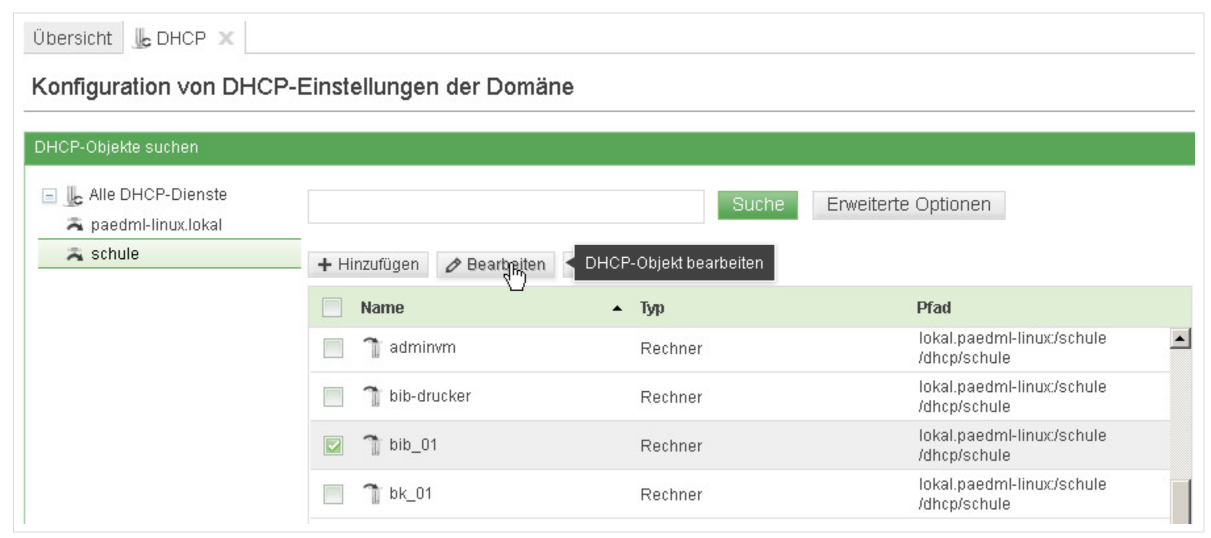


Abb. 79: Aufruf des soeben geänderten Rechners

Im Reiter „*Richtlinien*“ und dort im Abschnitt „*Richtlinie: DHCP-Boot*“ wurde durch die Änderung der IP-Adresse eine Änderung vorgenommen, die nun manuell rückgängig gemacht werden muss. Der Eintrag „*Ererbt*“ im Feld „*Richtlinien-Konfiguration*“ wird systemseitig gesetzt. Dadurch bekommt der Rechner einen falschen „*Boot-Server*“ gesetzt und der „*Boot-Dateiname*“ wird u.U. ebenfalls falsch eingetragen.

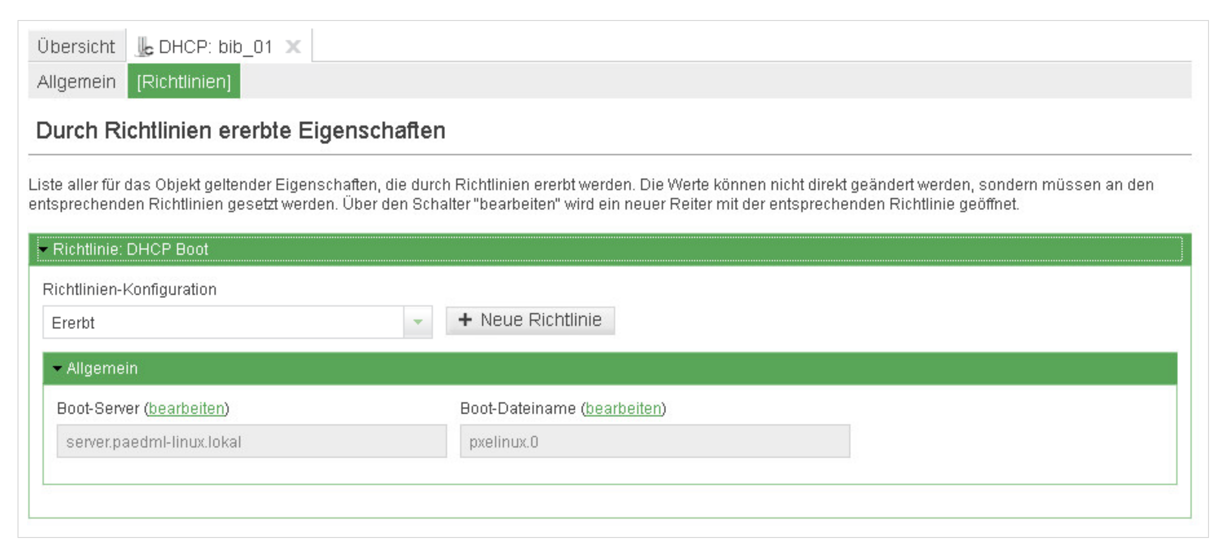


Abb. 80: Reiter-„Richtlinien“ | Abschnitt „Richtlinie: DHCP-Boot“ mit falschen Werten

Ändern Sie den Eintrag im Feld „Richtlinien-Konfiguration“ über das Drop-Down-Menü. Hier muss – abhängig von der Firmware-Variante des Gerätes – einer der folgenden Einträge gewählt werden:

- Wählen Sie „cn=opsi-boot,cn=boot,…“, wenn es sich um einen Rechner mit BIOS handelt.
- Wählen Sie „cn=opsi-uefi-boot,cn=boot,…“, wenn es sich um einen Rechner mit UEFI handelt.

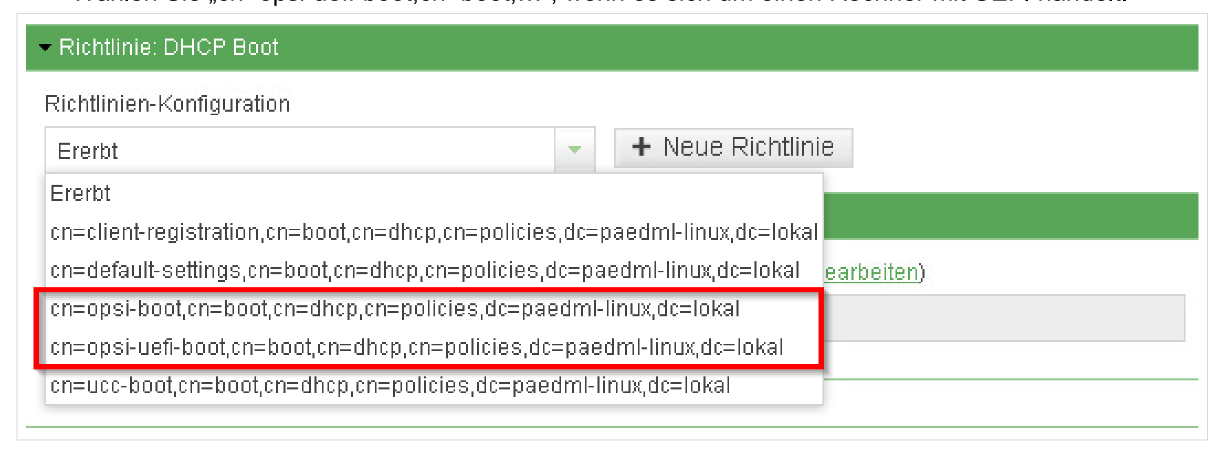


Abb. 81: Auswahl der Richtlinie – abhängig von der Firmware-Variante des Rechners

Wenn Sie die Änderung vorgenommen haben, dann werden die Einträge in den Feldern „*Boot-Server*“ und „*Boot-Dateiname*“ automatisch an die richtigen Werte angepasst. Übernehmen Sie die Einstellungen mit „*Änderungen speichern*“.

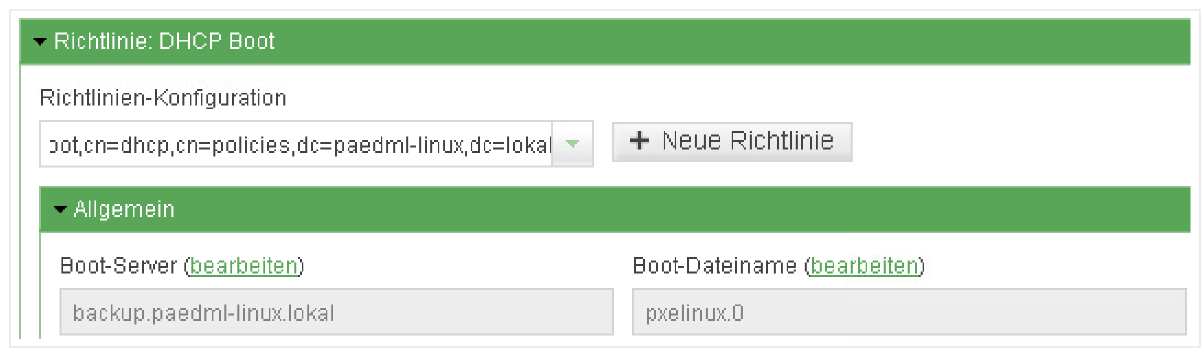


Abb. 82: Reiter-„Richtlinien“ | Abschnitt „Richtlinie: DHCP-Boot“ mit richtigen Werten für BIOS-Rechner

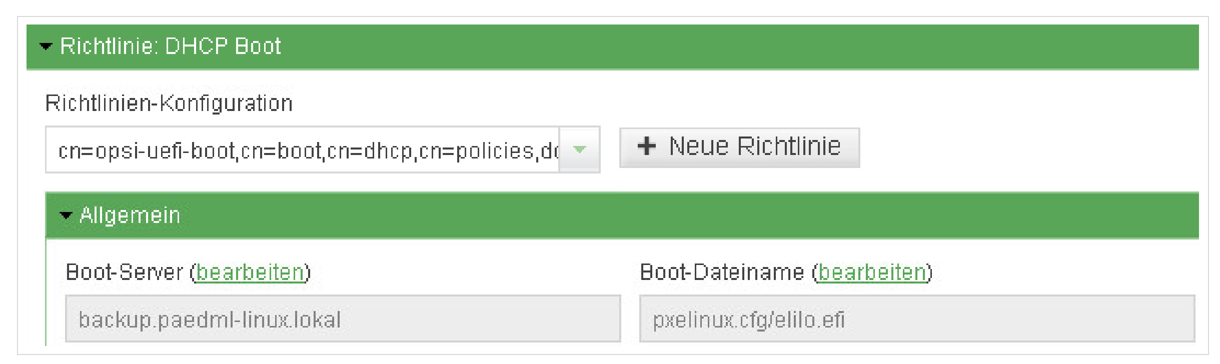


Abb. 83: Reiter-„Richtlinien“ | Abschnitt „Richtlinie: DHCP-Boot“ mit richtigen Werten für UEFI-Rechner

5. Verwaltung der Computerräume

Aufruf über Schulkonsole: Schul-Administration | Computerräume verwalten



Bitte beachten Sie unbedingt die Hinweise zur Nomenklatur der *paedML Linux* im Anhang A, Seite 295.

Um neue Computerräume hinzuzufügen, melden Sie sich als Netzwerkberater an der *Schulkonsole* an.

Im Menü „*Schul-Administration* | *Computerräume verwalten*“ werden die in Kapitel 4 angelegten Geräte der Schule einem Computerraum zugeordnet. Diese Computerräume können von den Lehrern während des Unterrichts verwaltet werden, etwa indem der Internetzugang freigegeben wird.

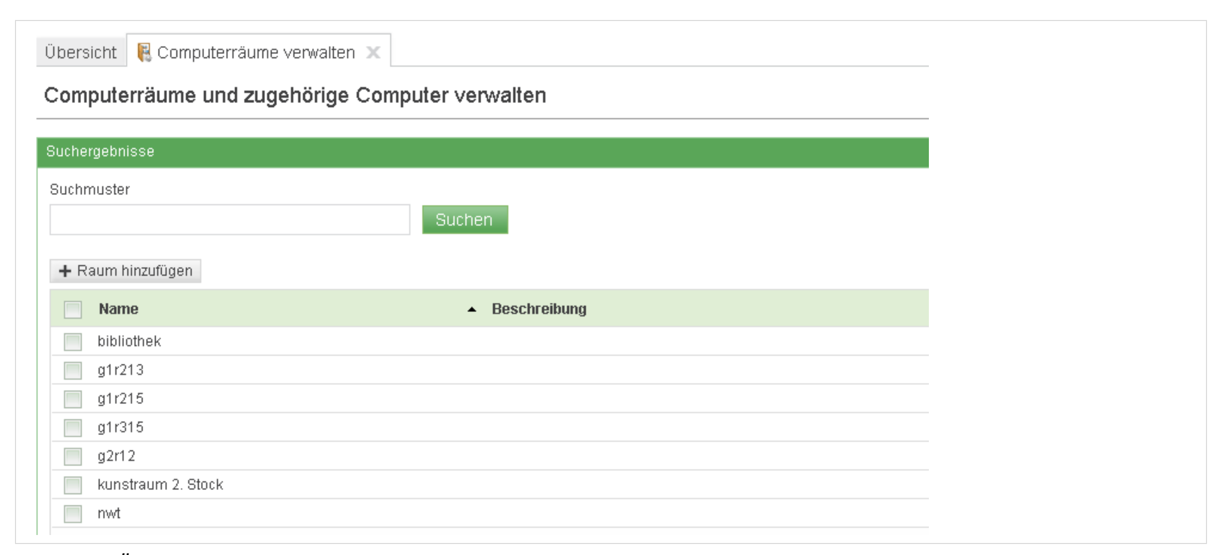


Abb. 84: Übersicht über die Computerräume

5.1 Anlegen von Computerraum und Zuweisung von Geräten



Es gibt keine Überprüfung, ob ein Computer bereits einem Raum zugeordnet wurde, daher können Rechner verschiedenen Räumen zugewiesen werden. Dies sollte nach Möglichkeit vermieden werden!

Andernfalls erscheinen die Rechner in verschiedenen Computerräumen und Lehrende könnten sich bei der Bedienung der Schulkonsole in die Quere kommen. Wenn beispielsweise beim Unterrichten in Raum A ein Client gesperrt wird, der in Raum B steht und beiden Räumen zugewiesen ist, würde der Client (ohne Wissen der Lehrkraft in Raum B) gesperrt werden.

Mit dem Knopf “*Raum hinzufügen*“ wird ein neuer Computerraum angelegt.

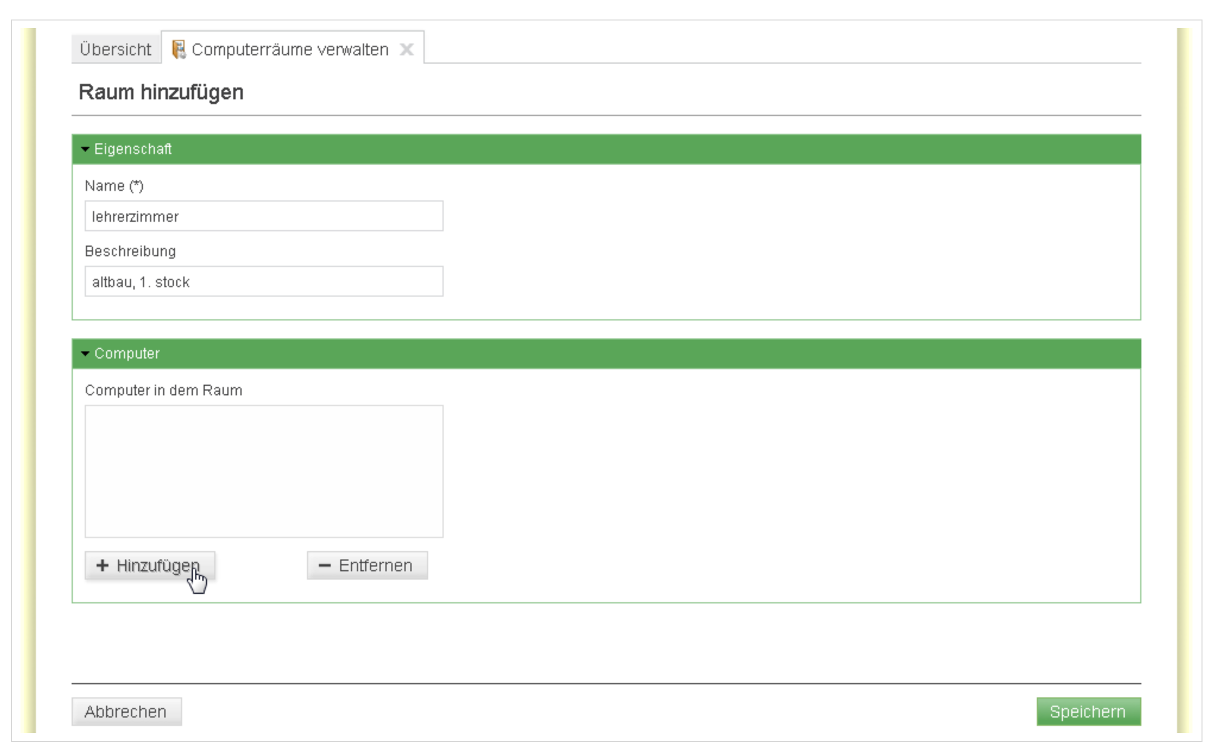


Abb. 85: Hinzufügen eines neuen Computerraumes

In der Maske „*Raum hinzufügen*“ werden im Abschnitt „*Computer*“ alle dem Raum zugewiesenen Computer angezeigt. Wenn Sie auf „*Hinzufügen*“ klicken, können Sie weitere Rechner hinzufügen.

Das sich öffnende Fenster „*Objekte hinzufügen*“ verfügt über eine Suchfunktion, über die Sie nach Computern suchen können. Die Eingabe von `*` (Stern) im Feld „*Suchmuster*“ und ein anschließender Klick auf „*Suchen*“ zeigt alle im System registrierten Geräte an. Wenn Sie einen Teil eines bekannten Namens eingeben, dann wird dieser Suchstring gesucht. Am folgenden Beispiel wird im System nach Geräten gesucht, die im Namen den Suchstring „*lehr*“ (Lehrerzimmer) haben.

Wählen Sie aus, welche Objekte in den Raum aufgenommen werden sollen und klicken Sie anschließend auf „*Hinzufügen*“.



Abb. 86: Zuweisen von Geräten zu einem Computerraum

Wenn die Bearbeitung eines Computerraumes abgeschlossen ist, wird das Ergebnis gespeichert, damit die Änderungen aktiv werden.

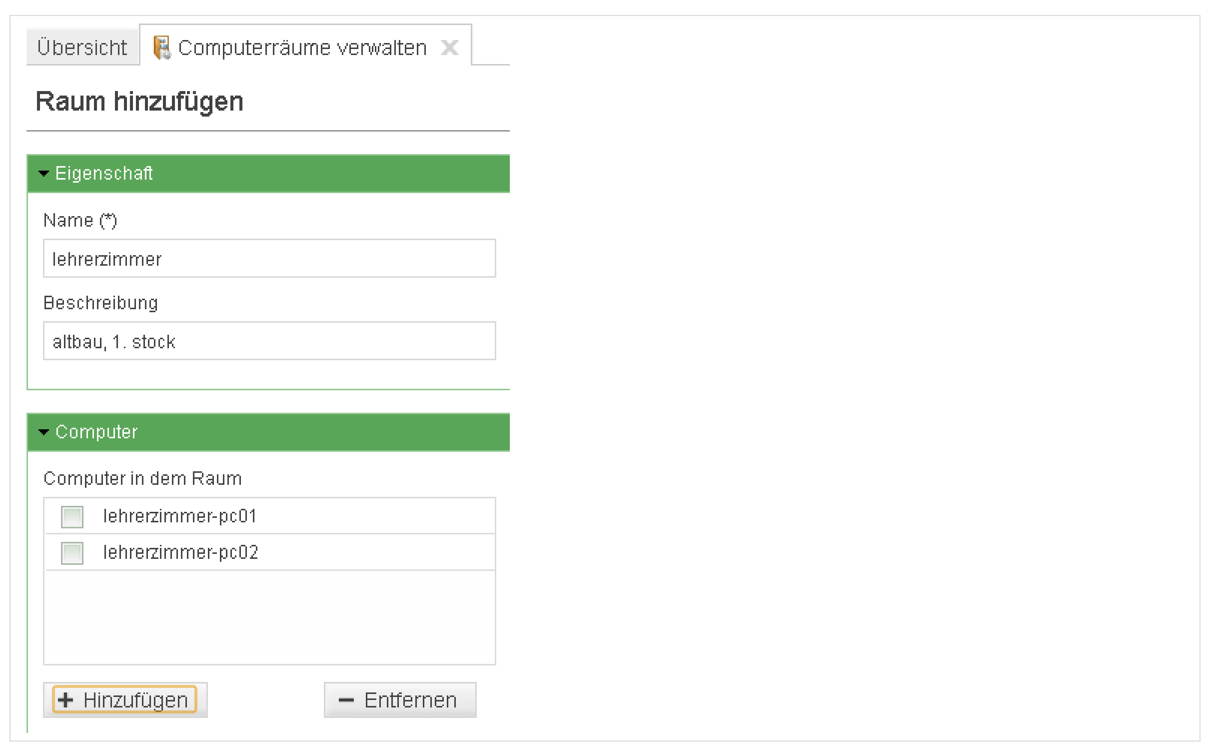


Abb. 87: Der neu angelegte Raum Lehrerzimmer mit allen darin befindlichen Clients

5.2 Entfernen vor Rechnern aus Computerräumen

Wenn Sie Rechner aus einem Raum löschen wollen, dann wählen Sie den jeweiligen Raum in der Übersicht der Computerräume aus. Anschließend aktivieren Sie die Checkbox vor dem Rechnernamen (Auswahl mehrerer Objekte möglich). Ein Linksklick auf „*Entfernen*“ löscht die ausgewählten Objekte aus dem Raum, das Gerät selbst wird dabei aber nicht gelöscht.

5.3 Entfernen von Computerräumen

Bereits angelegte Computerräume können nachträglich über die Computerraumverwaltung bearbeitet oder gelöscht werden. Aktivieren Sie in der Übersicht die Checkbox vor einem Raum und klicken Sie auf „*Löschen*“, um den Raum zu löschen. Es ist nicht möglich, mehrere Räume gleichzeitig zu löschen. Bevor der Löschvorgang ausgeführt wird, erscheint eine Abfrage, die bestätigt werden muss.

Die Geräte, die einem Raum zugeordnet sind, werden nicht gelöscht, wenn der Raum gelöscht wird.

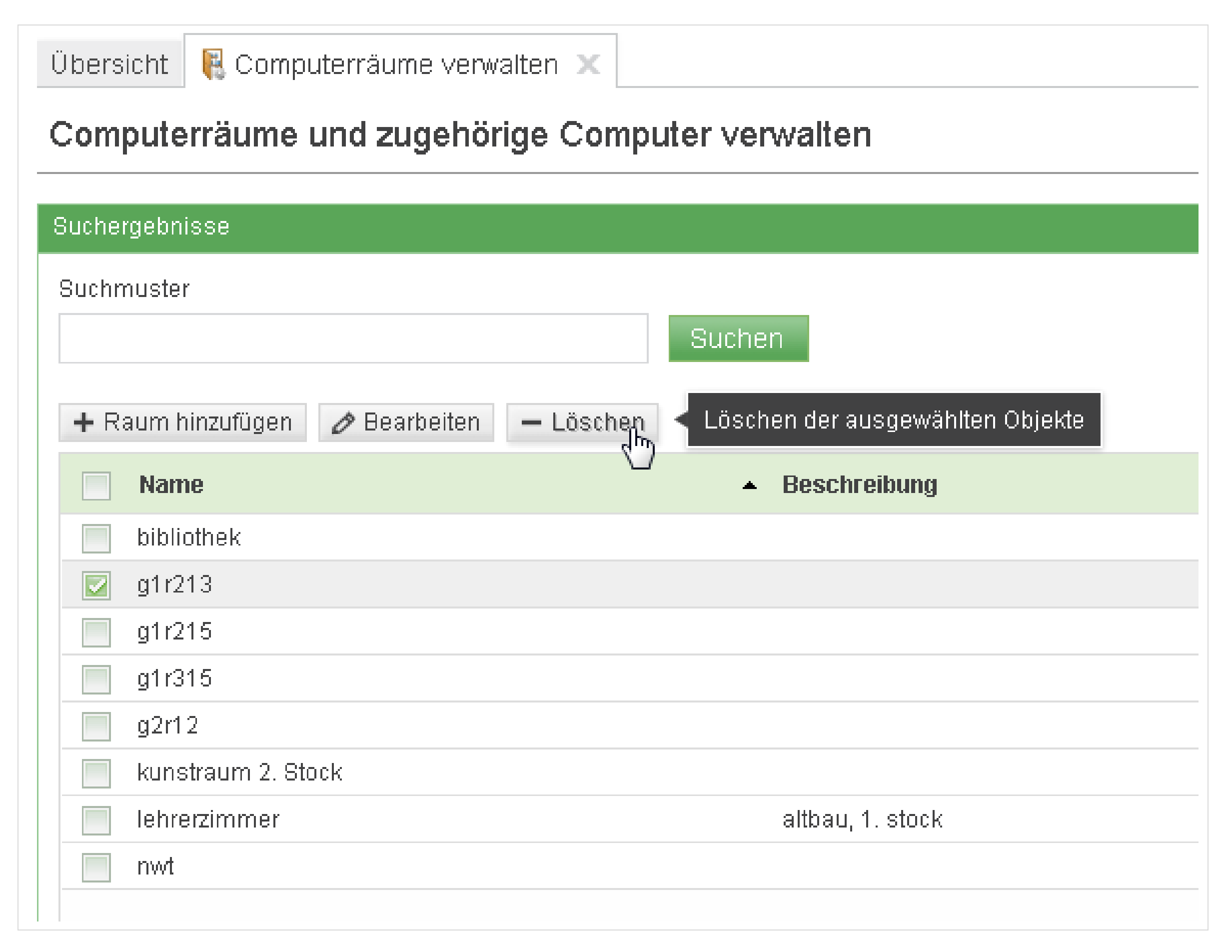


Abb. 88: Computerraum löschen

6. Einrichtung von Druckern

Bereitstellung von Druckertreibern via Samba
In der *paedML Linux* werden Druckaufträge über das Drucksystem *CUPS (Common Unix Printing System)* [31] ausgeführt. *CUPS* läuft als Systemdienst auf dem Server und dient als Warteschlange für die Verarbeitung von Druckaufträgen.

Beim Drucken spielt der Systemdienst *Samba* eine wichtige Rolle. Dort werden die Druckertreiber für die *Windows*-Rechner hinterlegt. Dies geschieht über die *Windows*-Freigabe „*print$*". Jede Druckerfreigabe wird mit Hilfe des von *Windows* bereitgestellten *Point 'n' Print* Verfahrens mit einem Treiber aus der „*print$*"-Freigabe verknüpft.

Über eine Zuordnung in der Schulkonsole bekommen Computerräume Drucker zugewiesen. Bei der Einrichtung der Computer wird – sofern ein Drucker zugewiesen ist – automatisch der Druckertreiber für den Client bereitgestellt. Hierdurch kann der Benutzer auf den entsprechenden Drucker zugreifen und über die Druckerfreigabe drucken.

Druckprozess
Nachdem die Druckertreiber auf dem Client installiert wurden, kann der Druckauftrag an den Drucker (bzw. die Druckerfreigabe) versandt werden (1). *Windows*clients erkennen hierbei den Druckdienst CUPS an der von Samba bereitgestellten Druckerfreigabe und übertragen die Druckdaten an CUPS (2). Alle ankommenden Druckaufträge werden von CUPS in einer Warteschlange abgearbeitet und an die Drucker weitergeleitet (3).

Die folgende Grafik zeigt Ihnen schematisch wie das Drucken der *paedML Linux* funktioniert.

---

[31] http://de.wikipedia.org/wiki/Common_Unix_Printing_System

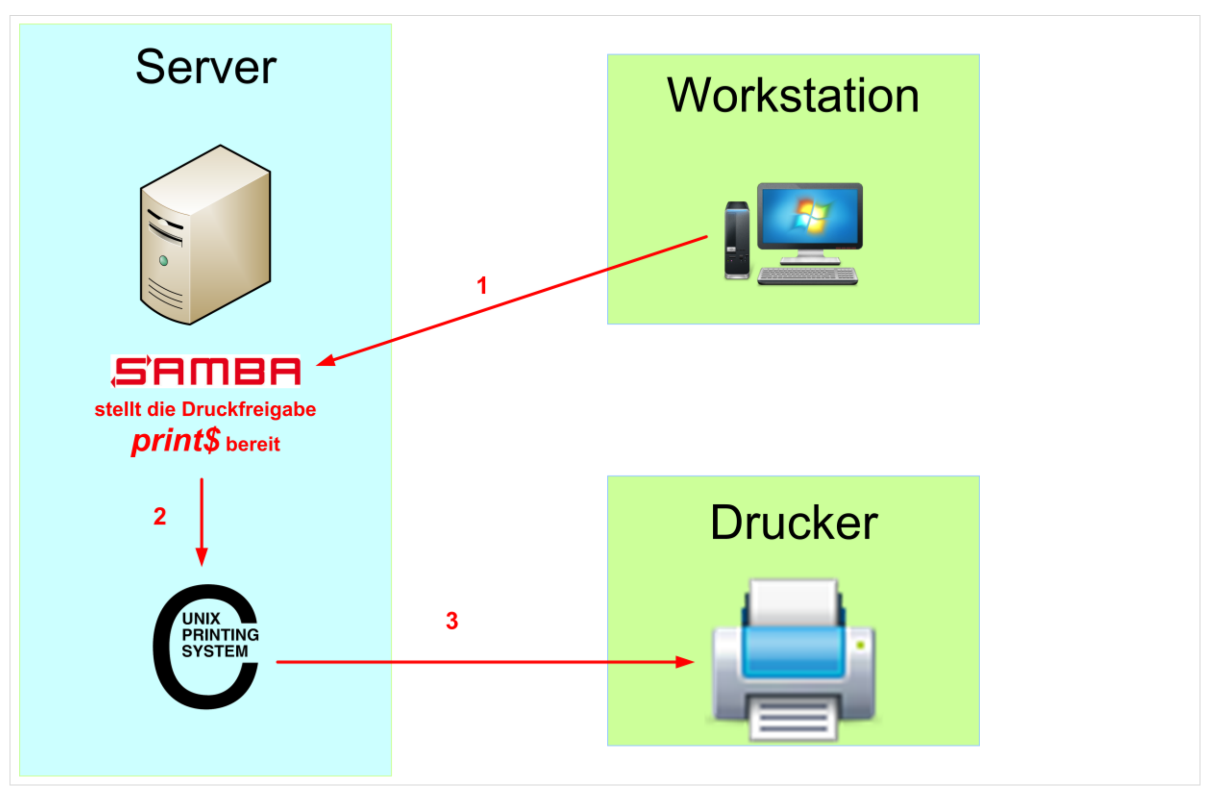


Abb. 89: Überblick über die Verwaltung von Druckaufträgen



Achten Sie bei der Anschaffung von Druckern darauf, dass diese netzwerkfähig sind und möglichst ein netzwerkfähiger Treiber zur Verfügung steht.

(*Optional, wenn auch Linux-Clients zum Einsatz kommen:*

Achten Sie bei der Anschaffung von Druckern unbedingt darauf, dass diese mit Cups betrieben werden können. Es gibt Geräte, für die keine Treiber für Linux zur Verfügung stehen.

Eine Integration solcher Geräte in *CUPS* ist – wenn überhaupt – nur mit erheblichem Aufwand umsetzbar[32].)

Es wird ausdrücklich empfohlen Drucker via Netzwerkkabel an das Schulnetz anzuschließen und am Server einzurichten.

Die in Kapitel 6.7, Seite 113, beschriebene Möglichkeit Drucker direkt an einem Arbeitsplatzrechner anzuschließen und über eine lokale Druckerfreigabe zu drucken wird nur als Notlösung beschrieben, aber nicht durch die Hotline unterstützt.

[32] Informationen zur Unterstützung durch CUPS und – sofern verfügbar – Treiber gibt es bei http://www.linuxprinting.org

Übersicht

- Zunächst wird in diesem Kapitel beschrieben, wie Sie – analog zu Kapitel 4.2.3 „Rechneraufnahme über die Schulkonsole“ – einen Drucker in das pädagogische Netzwerk aufnehmen.
- Im Anschluss wird das Anlagen eines Druckers über die Druckverwaltung beschrieben (Kapitel 6.2).
- Die Integration weiterer Druckertreiber, die nicht in Cups enthalten sind, wird in Kapitel 6.3 beschrieben. Dieses Kapitel kann in der Regel übersprungen werden und ist nur relevant, wenn Sie die Druckermoderation aktivieren.
- Kapitel 6.4 zeigt auf, wie die Druckermoderation eingerichtet wird.
- Darauf folgt ein Unterkapitel (Kapitel 6.5) zur Bereitstellung von Treibern über *Samba*.
- Die Druckerzuordnung an bestimmte Räume ist Gegenstand von Kapitel 6.6.
- Im darauf folgenden Kapitel 6.7 wird die manuelle Einrichtung von Druckern an einzelnen Arbeitsplätzen beschrieben.
- Das Kapitel endet mit Hinweisen zum PDF-Drucker, über den Benutzer in PDF-Dateien drucken können (Kapitel 6.8).

Checkliste: Ablauf der Druckereinrichtung

Die Einrichtung eines Druckers geschieht in vier Schritten:

- ☐ Integration des Druckers in die Domäne.
- ☐ Anlegen/Einrichten des Druckers im Drucker-Modul der Schulkonsole.
- ☐ Einrichtung der Treiber in der Samba-Domäne.
- ☐ Zuweisung der Drucker an Räume, damit der Druckertreiber an die Clients verteilt werden kann.

6.1 Integration des Druckers in die Domäne

Aufruf über Schulkonsole: Schul-Administration | Computer hinzufügen.
Bevor das Druckerprofil im System eingerichtet werden kann, muss das zugehörige Gerät (Drucker oder Printserver) in die paedML aufgenommen werden. Dies geschieht als *Administrator* über die Rechnerverwaltung in der *Schulkonsole* im Menü „*Schul-Administration* | *Computer hinzufügen*“.

Gehen Sie hierbei wie in Kapitel 4.2.3 „Rechneraufnahme über die Schulkonsole“, Seite 77 beschrieben vor. Der Unterschied zur Aufnahme eines Rechners liegt darin, dass für Drucker kein Computerkonto erstellt wird.

Sie wählen also in der Maske, in der der Computertyp definiert wird, den letzten Eintrag „*Gerät mit IP-Adresse*“. Dieser ist für Netzwerkgeräte – in diesem Fall ein Drucker. Anschließend wird für das Gerät eine DHCP-Adresse reserviert und ein DNS-Eintrag erstellt.

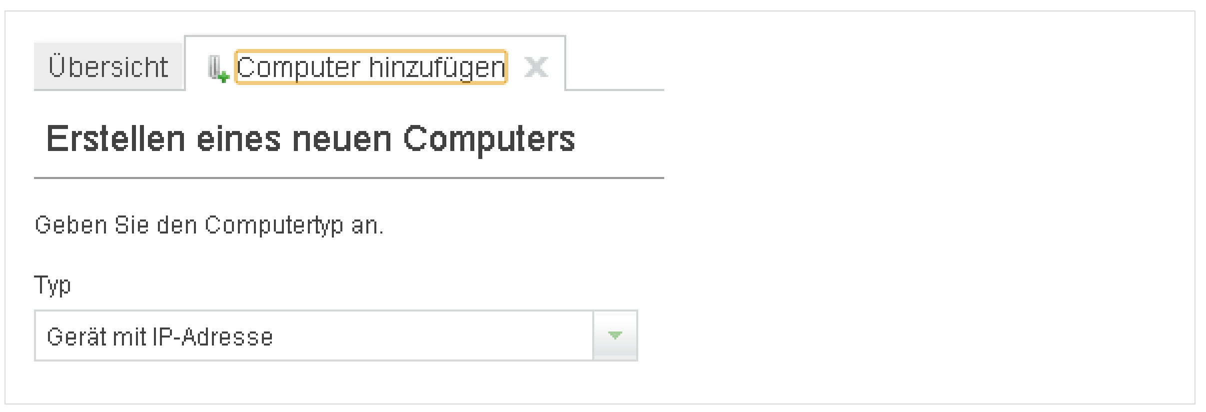


Abb. 90: Drucker haben den Typ Gerät mit IP-Adresse, sonst ist die Einrichtung gleich wie in Kapitel 4.2.3

Wenn der Drucker in das Netzwerk aufgenommen wurde, muss das Gerät so konfiguriert werden, dass es die in der *Schulkonsole* zugewiesene IP-Adresse erhält und dadurch im Netzwerk erreichbar ist. Das Gerät sollte hierfür so konfiguriert sein, dass es seine Netzwerkeinstellungen über DHCP bezieht. Nähere Informationen hierzu entnehmen Sie bitte dem Handbuch Ihres Druckers.



Falls der Drucker nicht über eine Netzwerkkarte verfügt, können Sie mit einem Druckserver (Printserver) arbeiten, der die Daten für den Drucker über ein Netzwerkkabel entgegen nimmt und an den Anschluss des Druckers weiterleitet.

6.2 Anlegen einer Druckerfreigabe

Aufruf über Schulkonsole (als Administrator): Domäne | Drucker
Die Verwaltung von Druckern geschieht ebenfalls über die *Schulkonsole*. Öffnen Sie hierfür den Menüpunkt "*Domäne* | *Drucker*" als *Administrator*. Sie erhalten eine Auswahl von im System hinterlegten Druckern (mindestens ein „*PDFDrucker*", der mit der *paedML Linux* ausgeliefert wird).

Beim Hinzufügen, Entfernen oder Bearbeiten einer Druckerfreigabe wird der Drucker automatisch auch in *CUPS* konfiguriert. Die Druckerfreigaben werden automatisch auch für *Windows*-Clients bereitgestellt. Dies geschieht mit dem Systemdienst *Samba*.

Über „*Hinzufügen*" können Sie einen neuen Drucker einrichten.

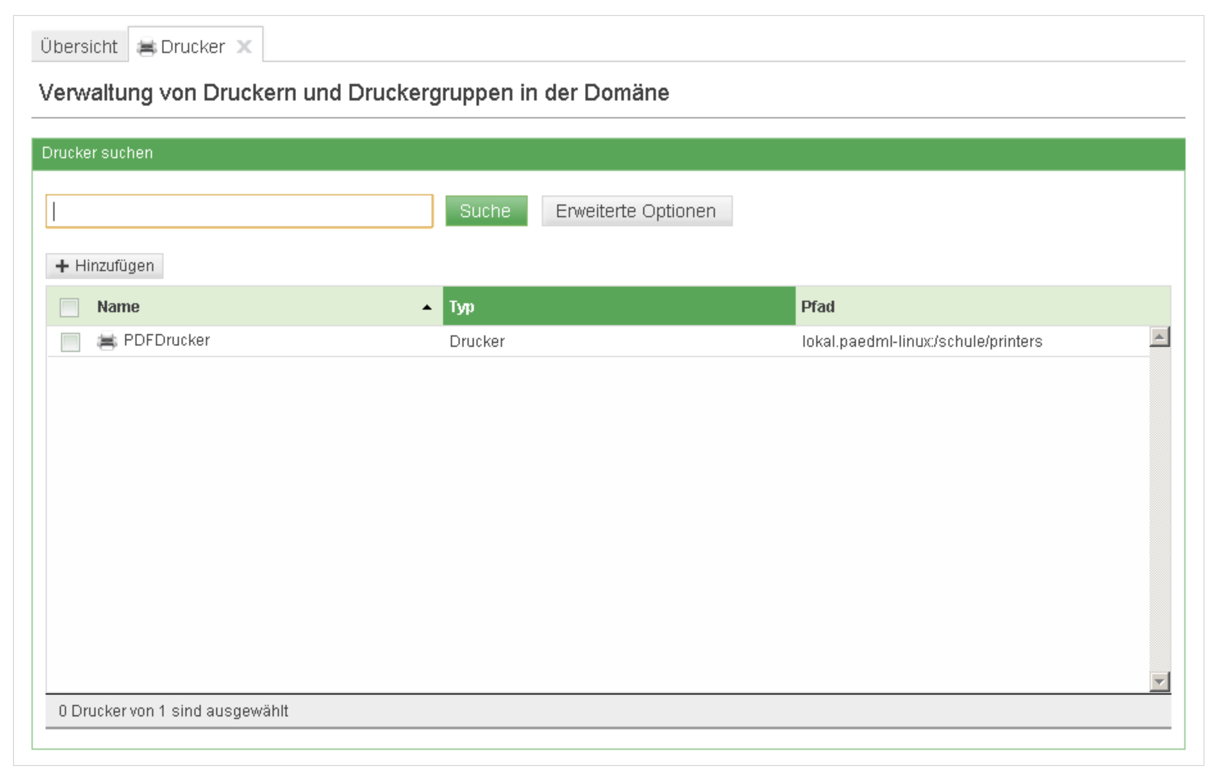


Abb. 91: Druckerverwaltung in der Schulkonsole

In den Einstellungen der nächsten Maske wählen Sie bitte unbedingt den „*Container lokal.paedml-linux/schule/printers*“ aus, damit der Drucker in der Schuldomäne verwaltet werden kann. Der Eintrag im Dropdownmenü „*Druckertyp*“ bleibt auf der Vorgabe „*Druckerfreigabe: Drucker*“. Weiter mit „*Weiter*“.

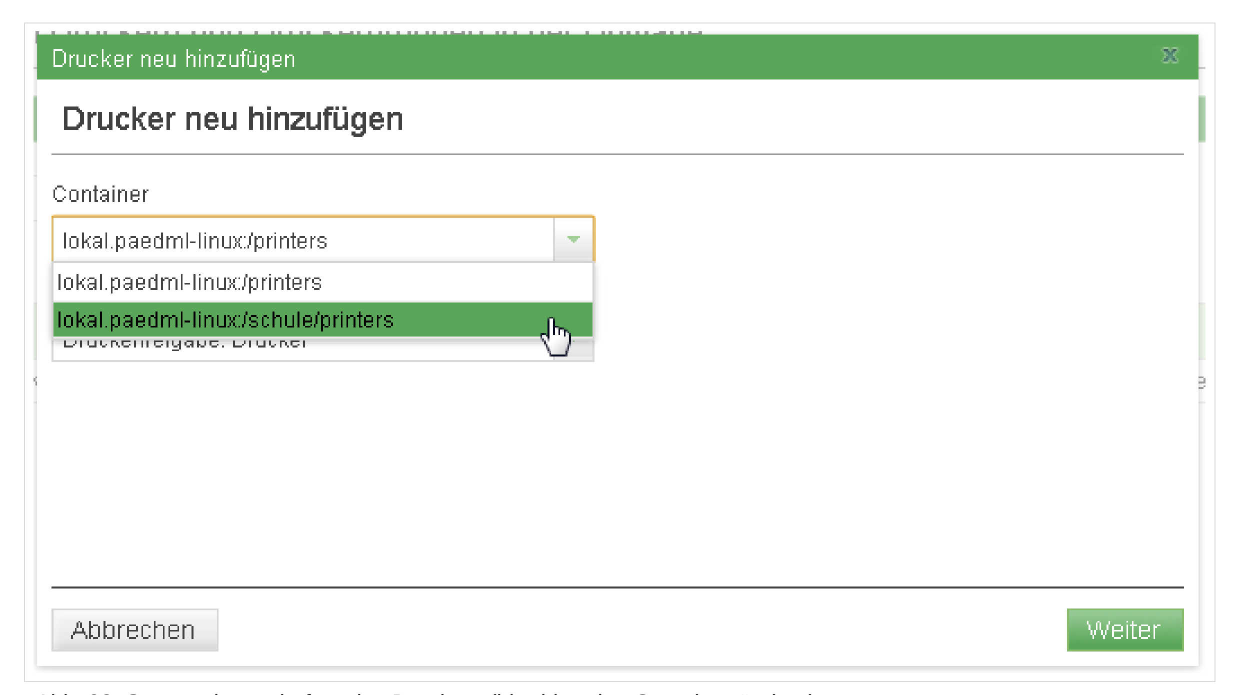


Abb. 92: Systemeigenschaften des Druckers (hier bitte den Container ändern)

Über die folgende Maske wird das Druckerprofil angelegt. Bitte tragen Sie hierbei die Werte ein, die für Ihren Drucker zutreffend sind. Die für die Konfiguration notwendigen Werte finden Sie in Tabelle 13:

Attribute für die Einrichtung eines Druckerprofiles (Attribute mit * müssen eingetragen werden) auf Seite 100.

Der Eintrag für „*Protokoll*“ ist davon abhängig, wie Sie den Drucker an das Netzwerk anschließen. Drucker, die an einer Netzwerkdose hängen, werden anders angesprochen als Drucker, die mit Computern verbunden sind. Das Protokoll ist in diesem Fall abhängig vom Drucker. Ältere Modelle nutzen häufig das „*Protokoll*“ „*socket://*“, neuere Modelle arbeiten meist mit dem „*Protokoll*“ „*http://*“.Entnehmen Sie bitte dem Handbuch des Druckers die genaue Protokollunterstützung.

Die IP-Adresse („*Ziel*“) entspricht dem Wert, den Sie bei der Aufnahme des Gerätes in die Domäne vergeben haben (Vgl. Kapitel 6.1 auf Seite 95).

Als Drucker-Hersteller sollten Sie den Wert „*misc*“ und als Modell den Wert „*None*“ eintragen.

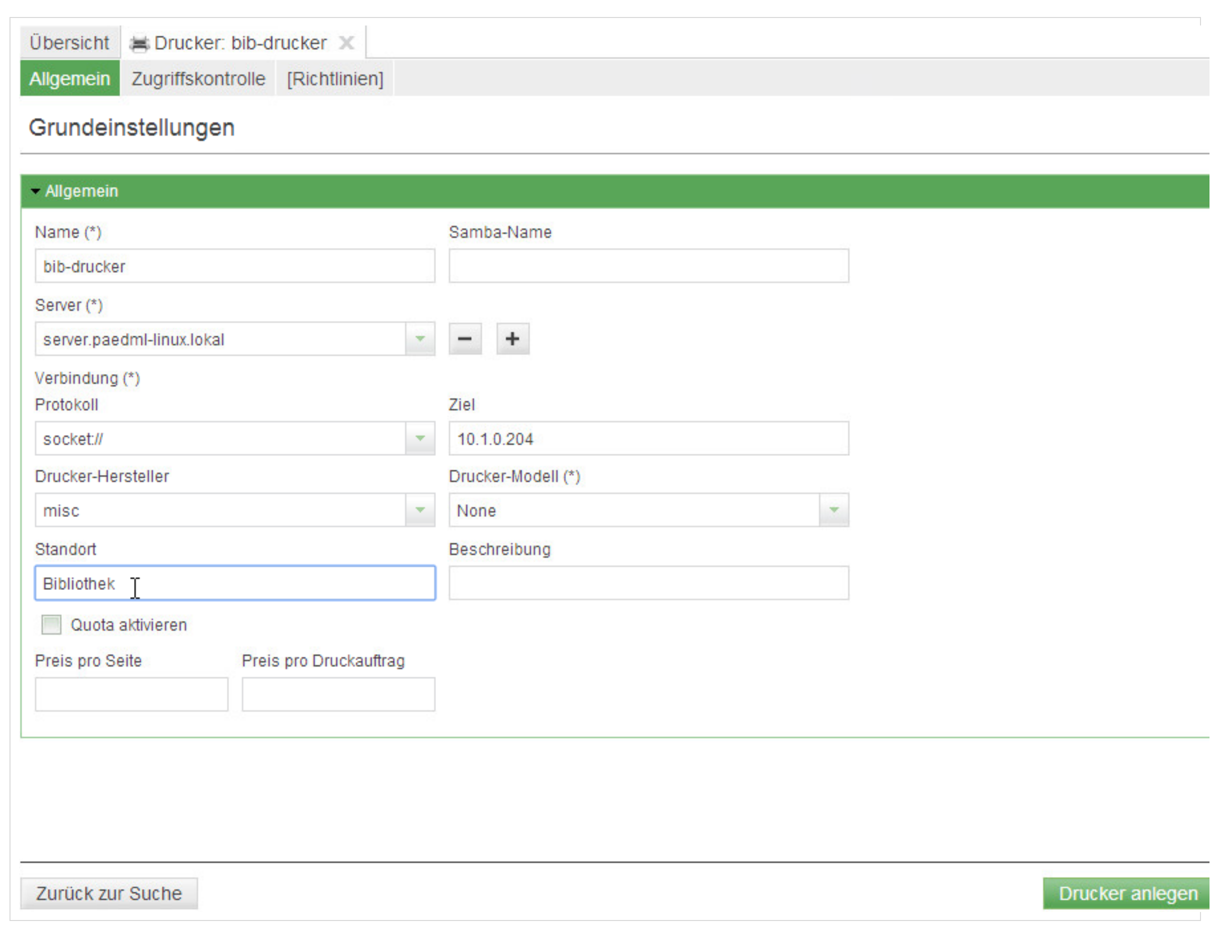


Abb. 93: Eingabe der Druckereinstellungen

Die folgende Tabelle gibt eine Übersicht über die einzelnen Felder, die in der Maske der Druckergrundeinstellungen vorhanden sind.

Attribut	**Beschreibung**
Name (*)	Dieses Feld enthält den Namen für die Druckerfreigabe. Dieses Feld wird nach dem Speichern gesperrt. Unter diesem Namen erscheint der Drucker unter *Windows* und Linux. Der Name der Druckerfreigabe darf nur Buchstaben und Zahlen sowie Binde- und Unterstriche enthalten.
Samba-Name	**Lassen Sie dieses Feld leer!**
Server (*)	Der Druckdienst **muss** auf dem Master-Server („*server*“) ausgeführt werden.
Protokoll und Ziel (*)	In diesem Feld wird definiert, wie der Druckserver auf den Drucker zugreift. Die folgende Liste beschreibt die Syntax der einzelnen Protokolle für die **Konfiguration lokal an den Server angeschlossener Drucker**: parallel://<devicedatei> Beispiel: parallel://dev/lp0 usb://<devicedatei> Beispiel: `usb://dev/usb/lp0` Die folgende Liste beschreibt die Syntax der einzelnen Protokolle für die **Konfiguration von Netzwerk-Druckern**: socket://<server>:<port> Beispiel: `socket://printer_03:9100` http://<server>[:<port>]/<pfad> Beispiel: `http://192.168.0.10:631/printers/remote` ipp://<server>/printers/<queue> Beispiel: `ipp://printer_01/printers/kopierer` lpd://<server>/<queue> Beispiel: `lpd://10.200.18.30/bwdraft` Das Protokoll „*cups-pdf*“ wird zur **Anbindung eines Pseudo-Druckers** verwendet, der aus allen Druckaufträgen ein PDF-Dokument erzeugt. Die Einrichtung ist in Abschnitt 6.8 auf Seite 114 dokumentiert. Das Protokoll „*file://*“ erwartet als **Ziel einen Dateinamen**. Der Druckauftrag wird nicht auf einen Drucker geschrieben, sondern in diese Datei, was für Testzwecke nützlich sein kann. Die Datei wird mit jedem Druckauftrag neu geschrieben.

	Mit dem Protokoll „***smb://***“ kann eine *Windows*-**Druckerfreigabe** eingebunden werden. Um beispielsweise die Druckerfreigabe laser01 des *Windows*-Systems win01 einzubinden, muss als Ziel win01/laser01 angegeben werden. Dabei sollten Hersteller und Modell-Typ entsprechend des verwendeten Geräts gewählt werden. Der Druckserver nutzt dabei die verwendeten Druckermodell Einstellungen um die Druckaufträge ggf. umzuwandeln und sendet diese anschließend an die URI `smb://win01/laser01`. Hierbei werden keine *Windows*-Treiber verwendet. Unabhängig von diesen Einstellungen kann die Druckerfreigabe auch weiterhin von anderen *Windows*-Systemen mit den entsprechenden Druckertreibern eingebunden werden.
Drucker-Hersteller (*)	Wählen Sie einen Hersteller, um die Auswahlliste in „*Druckermodell*“ zu aktualisieren. In Umgebungen, in denen weder Linux-Rechner noch die Druckermoderation zum Einsatz kommen ist der empfohlene Wert: „*misc*“
Drucker-Modell (*)	Hier werden alle verfügbaren *PPD*-Dateien des unter „*Drucker-Hersteller*“ ausgewählten Herstellers angezeigt. In Umgebungen, in denen weder Linux-Rechner noch die Druckermoderation zum Einsatz kommen ist der empfohlene Wert: „*None*“
Quota aktivieren	Wurden Quota für den Drucker aktiviert, greifen die Quota-Einstellungen der Richtlinie [Druck-Quota]. Hierfür muss das Druck-Quota-System installiert sein. **Derzeit wird die Druckqouta nicht durch die Hotline unterstützt.**
Preis pro Druckauftrag	Die anfallenden Kosten werden im Konto jedes Benutzers aufsummiert und dienen zur genauen Abrechnung von Druckkosten. Wird kein Wert angegeben, findet keine Druckkostenberechnung statt. Hierfür muss das Druck-Quota-System installiert sein.
Standort	Diese Angabe wird von einigen Anwendungen bei der Druckerauswahl angezeigt. Sie kann mit einem beliebigen Text gefüllt werden.
Beschreibung	Diese Angabe wird von einigen Anwendungen bei der Druckerauswahl angezeigt. Sie kann mit einem beliebigen Text gefüllt werden.

*Tabelle 13: Attribute für die Einrichtung eines Druckerprofiles (Attribute mit * müssen eingetragen werden)*

6.3 Integration weiterer Druckertreiber in CUPS

Aufruf über Schulkonsole (als Administrator): Domäne | LDAP-Verzeichnis
Die technischen Fähigkeiten eines Druckers werden in sogenannten *PPD-Dateien* spezifiziert. In diesen Dateien ist beispielsweise festgehalten, ob ein Drucker farbig drucken kann, ob ein beidseitiger Druck möglich ist, welche Papierschächte vorhanden sind, welche Auflösungen unterstützt und welche Druckerbefehlssprachen unterstützt werden (z.B. PCL oder Postscript).

Neben den bereits im Standardumfang enthaltenen *PPD-Dateien* können weitere über die *Schulkonsole* hinzugefügt werden. Die *PPD-Datei* wird in der Regel vom Hersteller des Druckers bereitgestellt und muss auf dem Server in das Verzeichnis */usr/share/ppd* kopiert werden.

Laden Sie hierfür den Druckertreiber des Herstellers auf den Rechner herunter, mit dem Sie die Administration des Netzwerkes vornhehmen.



Leider können nicht alle Drucker unter *CUPS* eingerichtet werden. In diesem Fall ist ein Drucken über den Server häufig nicht möglich.

Diese Drucker können aber unter Umständen – ohne Zugriffskontrolle seitens der Lehrer – direkt am Client eingerichtet werden.

Öffnen Sie das Programm WinSCP (vgl. Kapitel 0 auf Seite 31) und melden Sie sich mit Ihren Zugangdaten (Benutzername: `root`, Adresse: *server* Port *22*) am Server an. Navigieren Sie auf der rechten Fensterseite in das Verzeichnis */usr/shar/ppd* . Sie können die Datei direkt in das Verzeichnis kopieren, ein bestehendes Unterverzeichnis nutzen oder ein neues Anlegen.

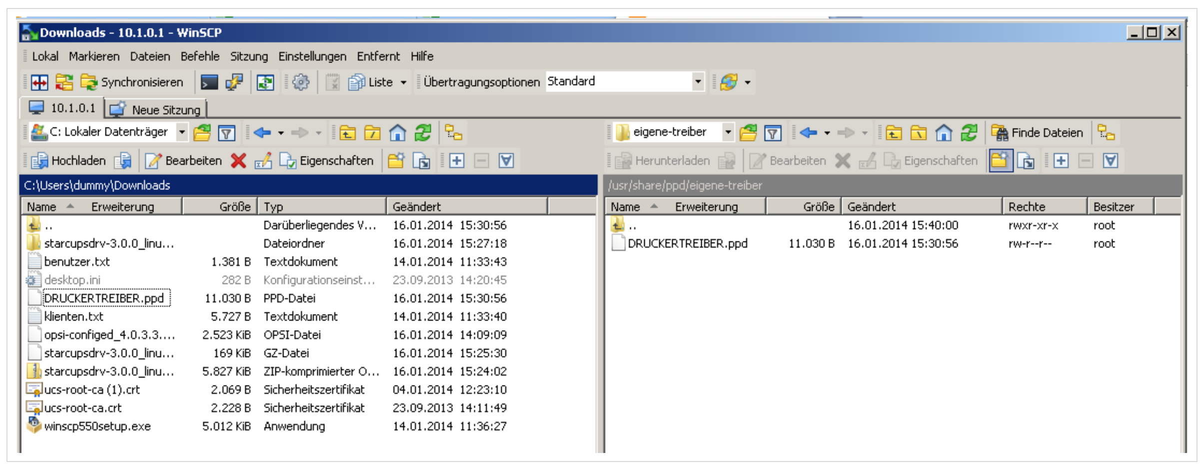


Abb. 94: In eigenes Verzeichnis hochgeladener neuer Druckertreiber

Die Druckertreiberlisten werden im Menü „*Domäne* | *LDAP-Verzeichnis*“ in der *Schulkonsole* verwaltet. Dort muss in den Container „*univention*“ und dort in den Untercontainer „*cups*“ gewechselt werden. Für die meisten Druckerhersteller existieren bereits Druckertreiberlisten. Diese können ergänzt werden.

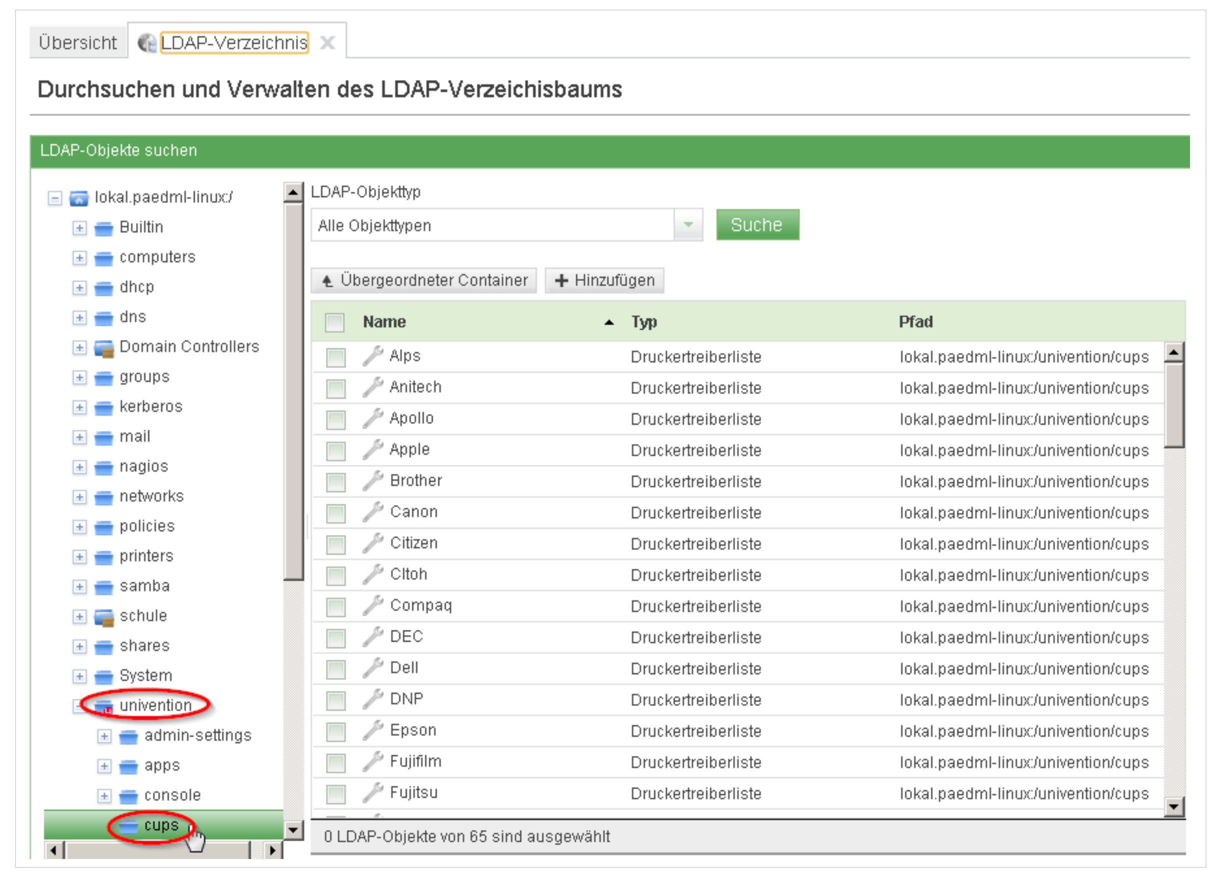


Abb. 95: LDAP-Container für Druckertreiber

Falls Sie ein Gerät haben, dessen Hersteller nicht in der Liste der Druckerhersteller ist, können Sie das Gerät entweder der Druckertreiberliste eines beliebigen anderen Herstellers zuordnen oder dem Objekt „*None*“, dass Sie zwischen den Herstellern „*NEC*“ und „*NRG*“ finden.

Wählen Sie den Namen der Druckertreiberliste, in die Sie den neuen Treiber hochladen wollen. Ein Klick auf den Namen öffnet die Liste der darin hinterlegten Drucker. Der unterste Eintrag der Liste sollte leer sein. Hier können Sie Ihren Neuen Drucker anlegen.

Der Pfad zur PPD-Datei, wird relativ zu dem Verzeichnis */usr/share/ppd/* eingetragen. Soll beispielweise die Datei */usr/share/ppd/eigene-treiber/DRUCKERTREIBER.ppd* verwendet werden, so ist hier „*eigene-treiber/DRUCKERTREIBER.ppd*“ einzutragen. Es können auch gzip-komprimierte Dateien (Dateiendung „*.ppd.gz*“) angegeben werden.

Drücken Sie auf „*Änderungen speichern*“, um den neuen Eintrag zu übernehmen

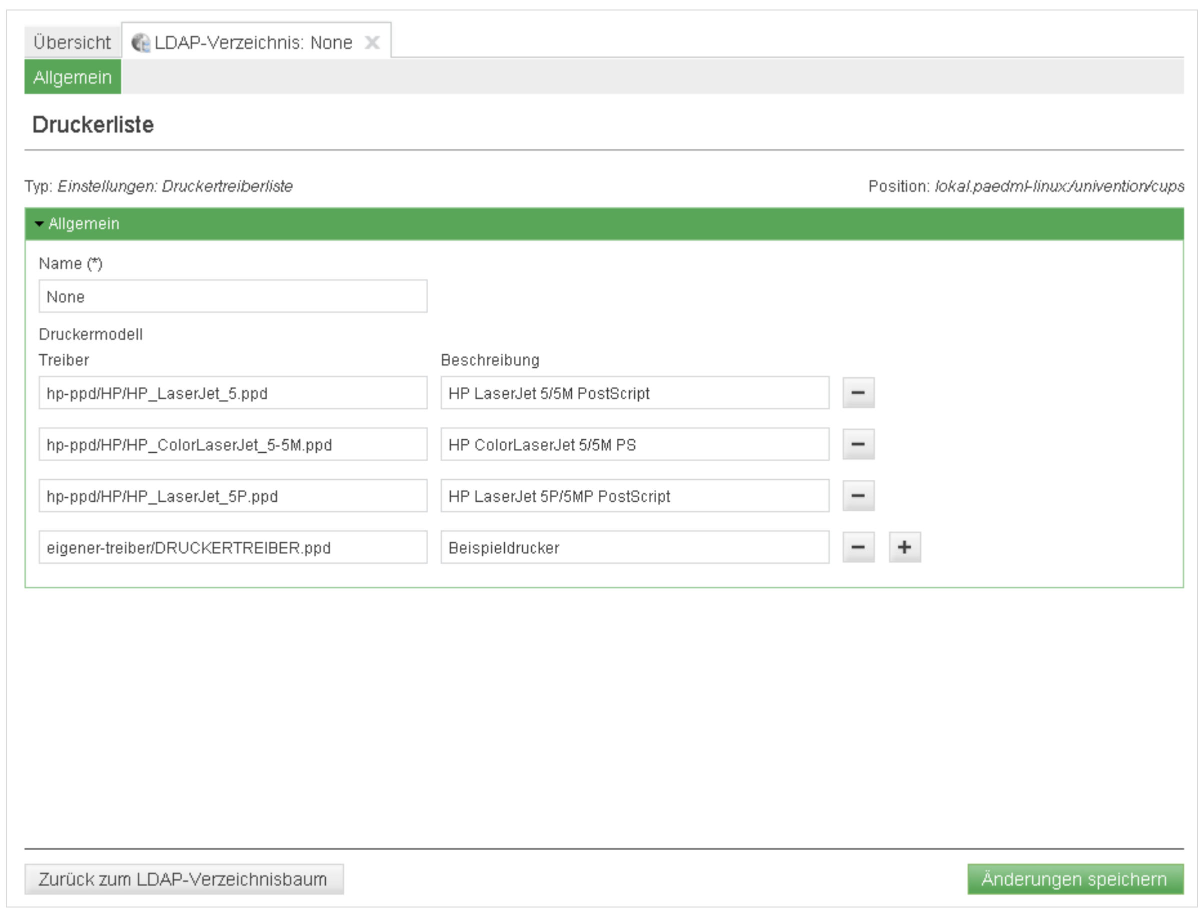


Abb. 96: Einbinden eines neuen Druckertreibers

Die folgende Tabelle beschreibt die einzelnen Felder:

Attribut	**Beschreibung**
Name (*)	Der Name der Druckertreiberliste. Unter diesem Namen erscheint die Liste in der Auswahlliste „Drucker-Hersteller“ auf der Karteikarte „Allgemein“ der Druckerfreigaben (Schulkonsolenmenü: „Domäne | Drucker“).
Treiber	Der Pfad zur PPD-Datei, relativ zu dem Verzeichnis /usr/share/ppd/. Soll beispielweise die Datei /usr/share/ppd/laserjet.ppd verwendet werden, so ist hier laserjet.ppd einzutragen. Es können auch gzip-komprimierte Dateien (Dateiendung .gz) angegeben werden.
Beschreibung	Eine Beschreibung des Druckertreibers, unter der er in der Auswahlliste Drucker-Modell auf der Karteikarte „Allgemein“ der Druckerfreigaben erscheint.

Tabelle 14: Integration neuer Druckertreiber

Nachdem der Druckertreiber im System hinterlegt wurde, kann er einem über das Schulkonsolenmodul „*Domäne* | *Drucker*“ einem Drucker zugewiesen werden.

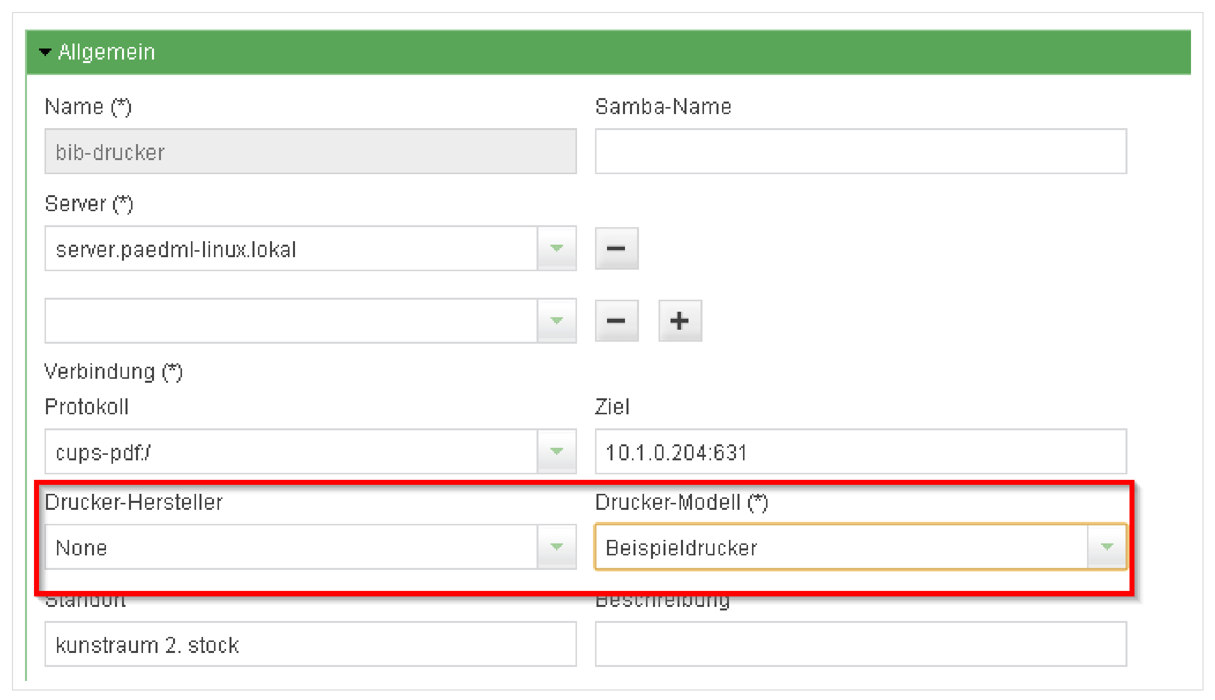


Abb. 97: Zuweisen des neuen Druckertreibers an einen Drucker

6.4 Vorbereitung der Druckermoderation

Die Druckermoderation wird im Handbuch für Lehrkräfte beschrieben. Wenn Sie eine Moderation von Druckaufträgen wünschen, dann wird empfohlen, dass Sie den zu moderierenden Drucker nicht für Schüler frei geben. Als Beispiel sei ein Farblaserdrucker genannt, der in einem Computerraum steht, aber ausdrücklich nur von Lehrkräften benutzt werden soll.

Wenn ein Schüler farbig drucken möchte, dann muss er im Fall der Moderation von Druckaufträgen einen -Druck (vgl. Kapitel 6.8, Seite 114) erstellen, der von der Lehrkraft ausgedruckt wird.



1. Druckermoderation bedeutet einen Mehraufwand für die Lehrkräfte, die Druckaufträge von Schülern durchschauen und frei geben müssen.
2. Wenn Sie die Druckermoderation nutzen wollen, benötigen Sie CUPS-, Treiber, die bei der Druckereinrichtung (vorheriger Abschnitt Felder: „*Drucker-Hersteller*“ und „*Drucker-Modell*“) im System ausgewählt werden müssen.



Eine weniger aufwändige Option, um Druckaufträge zu steuern bietet die Druckersperre der Schulkonsole, über die während des Unterrichts der Zugriff auf Drucker gesteuert werden kann.

Dieser Zugriff kann jedoch nicht so „fein“ gesteuert werden, wie die Druckermoderation.

Der zweite Reiter des Druckerprofils ermöglicht eine „*Zugriffskontrolle*“. Der Zugriff auf Drucker kann für einzelne Benutzer und für Gruppen geregelt werden. **Hier muss in der Regel nichts eingestellt werden.**

Attribut	Beschreibung
Zugriffslisten	Der Zugriff kann auf bestimmte Gruppen oder Benutzer beschränkt werden oder er kann generell freigegeben und spezifisch für bestimmte Gruppen oder Benutzer gesperrt werden. Diese Rechte werden auch für die entsprechende Samba-Druckerfreigabe übernommen.
Zugelassene/abgewiesene Benutzer	Diese Auswahl führt einzelne Benutzer auf, für die der Zugriff reguliert werden soll.
Zugelassene/abgewiesene Gruppen	Diese Auswahl führt Gruppen auf, für die der Zugriff reguliert werden soll.

Tabelle 15: Optionale Zugriffskontrolle auf Drucker

In den Standardeinstellungen dürfen alle Gruppen und Benutzer auf den Drucker zugreifen. Hierfür muss ein Drucker jedoch auf den Clients im Schulnetz eingerichtet werden.

Wenn Sie den Zugriff auf einen Drucker einschränken wollen, dann können Sie zwei Verfahren anwenden:

1. Sie können festlegen, dass **nur ausgewählte Benutzer oder Gruppen auf einen Drucker zugreifen dürfen**. Wechseln Sie hierfür in den Reiter „*Zugriffskontrolle*“ und wählen Sie im Dropdown-Menü den Eintrag „*Zugriff nur für ausgewählte Benutzer/ Gruppen zulassen*“. Im Anschluss können Sie Benutzer oder Gruppen in den dafür vorgesehenen Feldern „*Hinzufügen*“, die auf den Drucker zugreifen dürfen.

   In diesem Beispiel (siehe Screenshot) dürfen NUR Lehrer auf den Drucker zugreifen.
2. Sie können festlegen, dass der Zugriff **für ausgewählte Benutzer oder Gruppen verweigert** werden soll. Auch hierfür wechseln Sie in den Reiter „*Zugriffskontrolle*“. Wählen Sie im Dropdown-Menü den Eintrag „*Zugriff für ausgewählte Benutzer/ Gruppen verweigern*“. Im Anschluss können Sie Benutzer oder Gruppen in den dafür vorgesehenen Feldern „*Hinzufügen*“, die nicht auf den Drucker zugreifen dürfen.

Die neuen Einstellungen müssen jeweils mit „*Änderungen speichern*“ übernommen werden.

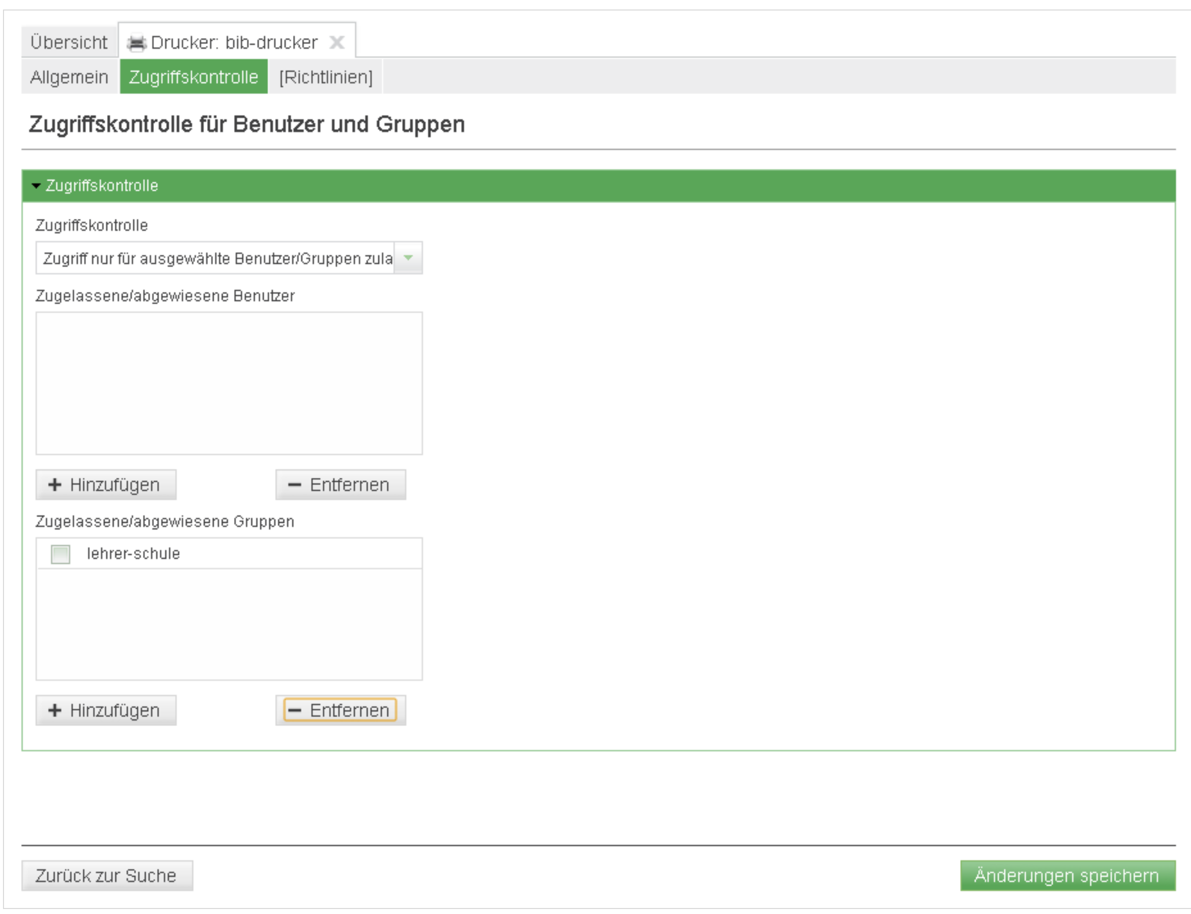


Abb. 98: Wer darf auf den Drucker zugreifen?



Durch dieses Verfahren kann nicht unterbunden werden, dass Benutzer, direkt über die IP-Adresse eines Druckers drucken.

Der dritte Reiter „*Richtlinien*“ ist nur dann relevant, wenn die Drucker-Quota aktiviert wird. Diese Funktion wird derzeit nicht von der Hotline unterstützt.

Wenn Sie alle Einstellungen vorgenommen haben, können Sie über den Knopf „*Drucker anlegen*“ den neuen Drucker anlegen. Dieser Drucker erscheint nun in der Übersicht der Druckerverwaltung.

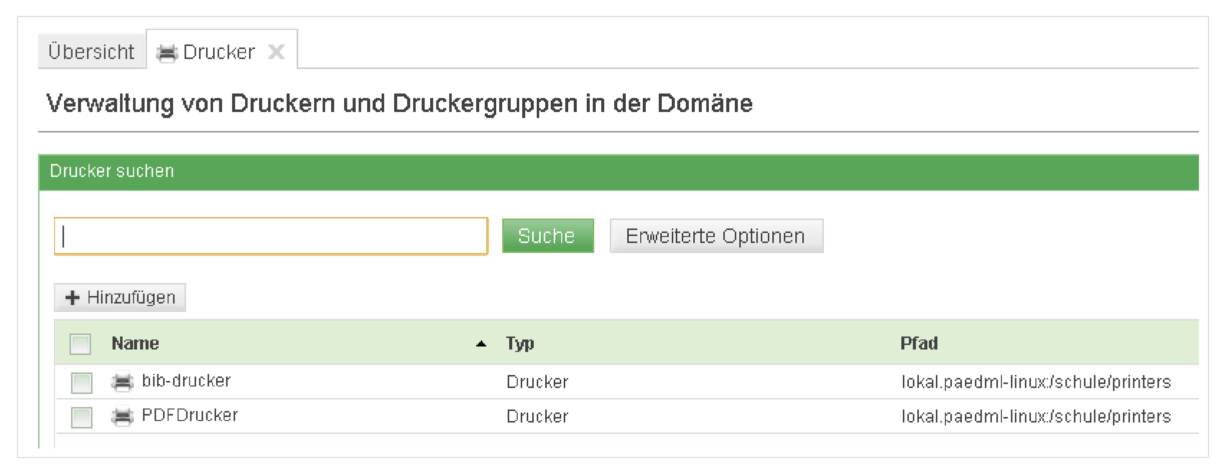


Abb. 99: Druckerverwaltungsmaske mit neu angelegtem Drucker

Um einen Drucker nachträglich zu bearbeiten, müssen Sie auf den „*Namen*“ des Druckers drücken. Sie gelangen in die Maske mit den „*Grundeinstellungen*“ des Gerätes.

6.5 Bereitstellen von Druckertreibern für Windows

Bei der Bereitstellung von Druckertreibern ist die Architektur der Client-Betriebssysteme relevant. Werden x86-(32-Bit)- *Windows*installationen, X64-(64-Bit)-*Windows*installationen oder beide parallel betrieben.

Es gibt also drei mögliche Szenarien:

1. *Reine 32-Bit Umgebungen* (auf den Rechnern, die drucken können sollen, ist jeweils nur *Windows*7 32-Bit (x86-Architektur) installiert):

   In diesem Fall muss auf dem Server mit dem Befehl

```
ucr set --force samba/global/options/spoolss:architecture="Windows x86"
```

   die Druckerfreigabe von Samba an die x86-Architektur angepasst werden. Bei der Treiberbereitstellung genügt es die Treiber für die x86-Architektur bereit zu stellen.

   Wenn auf eine Mischumgebung oder eine x64-Umgebung umgestellt wird, muss der Befehl

```
ucr unset --force samba/global/options/spoolss:architecture
```

   am Server ausgeführt werden.

2. *Reine 64-Bit Umgebungen* (die Rechner, die drucken können sollen, haben nur 64-bittige Betriebssysteme installiert):

   Hier genügt es die Druckertreiber als 64-Bit Version bereit zu stellen.

3. *Mischumgebungen von 32- und 64-bittigen Windowsinstallationen*:

   In einer gemischen x86/x64-Clientumgebung müssen generell immer für beide Architekturen die Treiber hochgeladen werden.

6.5.1 Druckertreiber auf der Samba-Freigabe hinterlegen

Windows unterstützt ein Verfahren zur serverseitigen Bereitstellung von Druckertreibern auf dem Druckserver (*Point 'n' Print*). Der folgende Abschnitt beschreibt die Bereitstellung der Druckertreiber unter *Windows* 7. Um die hier beschriebenen Schritte auszuführen, müssen Sie als Administrator der Domäne am *Windows*client angemeldet sein.

6.5.1.1 Vorgehensweise bei der Bereitstellung der Treiber



Die Benutzerführung unter Windows bietet zahlreiche Stolperfallen, es ist daher wichtig den einzelnen Schritten exakt zu folgen.

1. Zuerst müssen die Druckertreiber bereitgestellt werden. **Beachten Sei hierbei die vorausgehenden Hinweise zur Architektur**. Benötigt werden die *INF-Dateien* des Druckers. Diese werden in der Regel auf einem gesonderten Datenträger (Hersteller-CD) mit einem Drucker

ausgeliefert. Alternativ können die Dateien von der Homepage des Herstellers heruntergeladen werden.

2. Nachdem Sie sich die Dateien beschafft haben, starten Sie den *Windows Explorer* und öffnen Sie die „*Netzwerkumgebung*". Dort muss der „*Server*" (Netzwerk-Freigabe: *server*) ausgewählt werden, auf dem die Druckerfreigabe angelegt wurde. In der oberen Menüleiste wird nach einem Klick auf „*Remotedrucker anzeigen*" eine Liste mit allen Druckerfreigaben angezeigt.

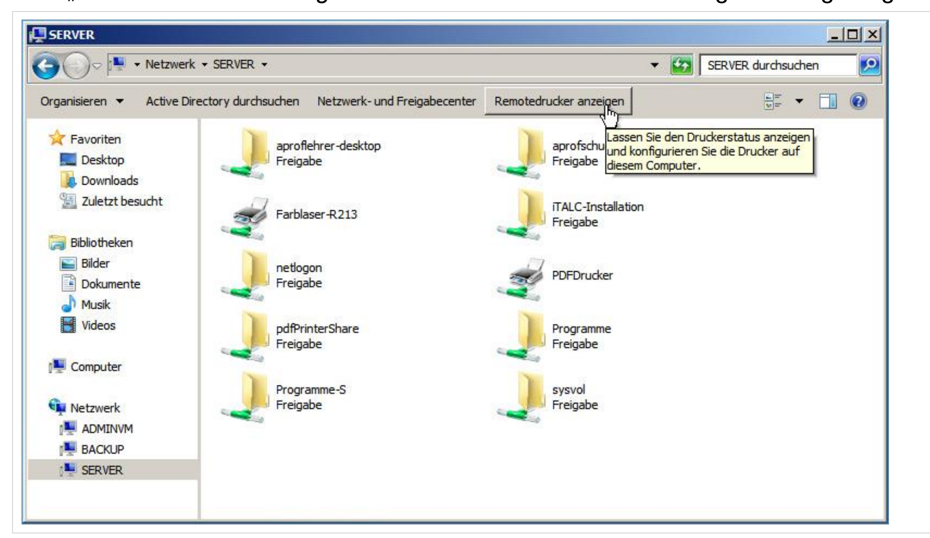


Abb. 100: Aufruf der Anzeige von Druckerfreigaben

3. Nun muss mit der rechten Maustaste auf die freie Fläche unter den Druckerfreigaben geklickt werden (**nicht auf eine der Freigaben, sonst öffnet sich das kontextsensitive Menü der Druckerfreigabe**) und „*Servereigenschaften*" gewählt werden. Dort im Reiter „*Treiber*" auf „*Hinzufügen*" drücken. Im folgenden Dialog auf „*Weiter*" drücken. In der nächsten Maske „*x86*" und/oder „*x64*"[33] auswählen „*Weiter*" drücken.

[33] Diese Auswahl ist davon abhängig, ob die Rechner auf einem 32(x86)-Bit oder einem 64(x64)-Bit Betriebssystem drucken sollen. (Siehe Hinweise vorheriger Abschnitt)

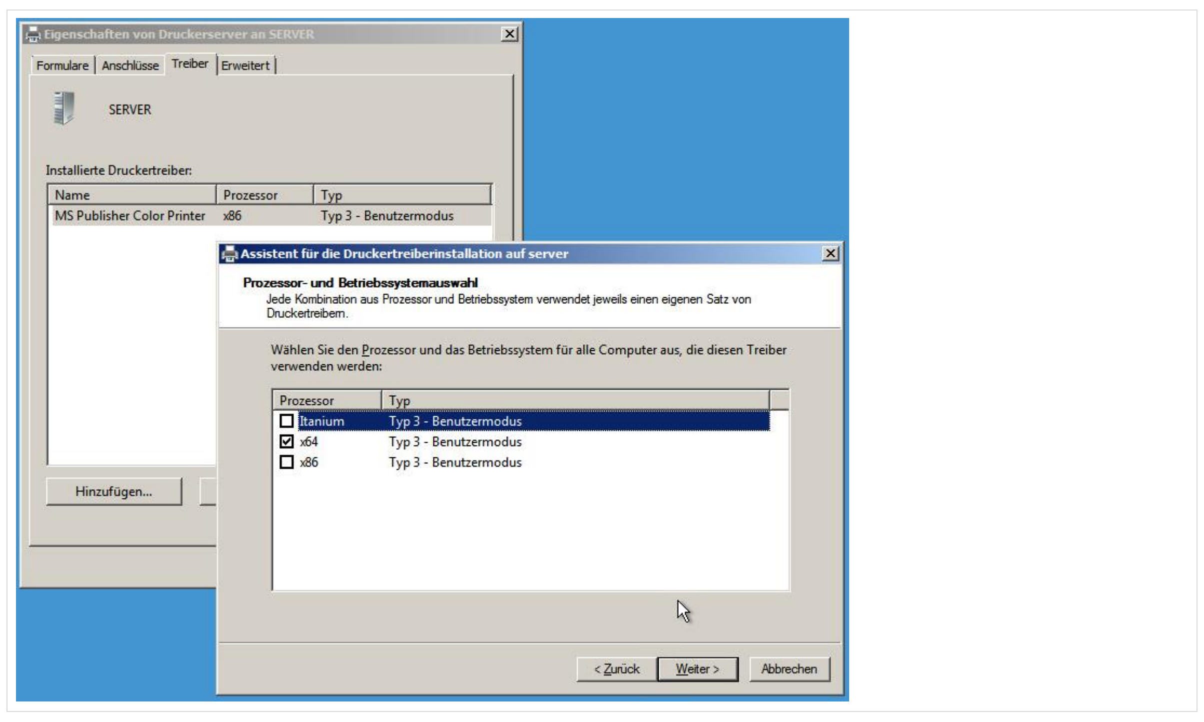


Abb. 101: Auswahl der Betriebssystem-Architektur

Um den neuen Treiber auf dem Server zu hinterlegen müssen Sie im nächsten Dialog auf „*Datenträger*" drücken und die Installationsquelle des Druckertreibers auswählen. Im sich dabei öffnenden Dateidialog müssen die INF-Dateien der Treiber (x86 und/oder x64) ausgewählt werden. Sie bestätigen die Auswahl einem Klick auf „*Weiter*" und schließen die Einrichtung mit einem Klick auf „*Fertig stellen*" ab. Danach werden die Treiber auf den Druckserver kopiert. Schließen Sie die Dialogfenster.

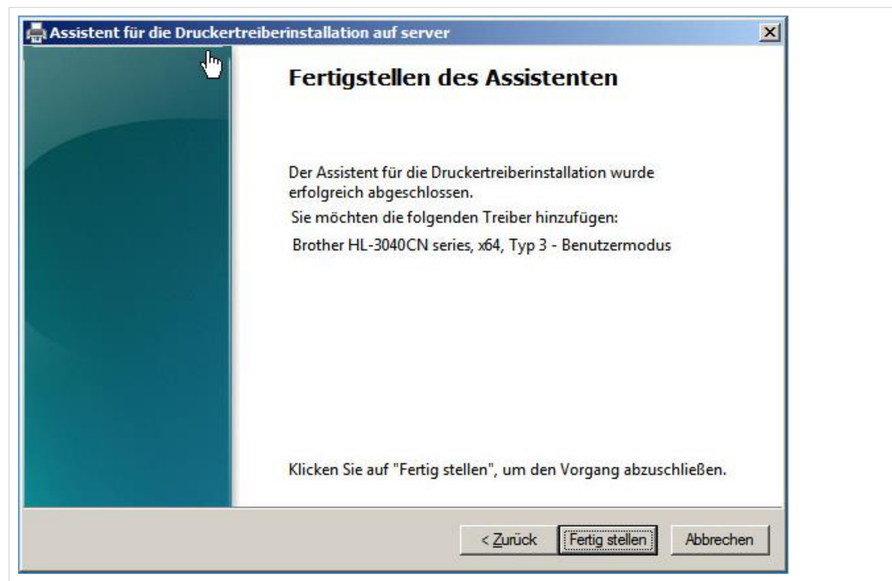


Abb. 102: Abschluss der Druckerinstallation

4. Nach diesen Schritten sind die Treiber auf dem Server im Verzeichnis */var/lib/samba/drivers* gespeichert.

5. Abschließend müssen sie den neu auf den Server kopierten Treiber mit dem Drucker verknüpfen.



1. Stellen Sie die Druckertreiber für ein Betriebssystem auf dem Server jeweils von einem Client mit dem gleichen Betriebssystem bereit. Es kommt zu einer Fehlermeldung, wenn zum Beispiel von einem *Windows-XP*-Client aus versuchen *Windows 7* Treiber zu installieren.
2. Der Druckertreiber für baugleiche Modelle muss nur einmal bereit gestellt werden. Die erneute Einrichtung des Druckertreibers führt zu einer Fehlermeldung, da der Treiber bereits installiert wurde. Im Fall baugleicher Drucker muss nach der einmaligen Treiberbereitstellung lediglich die Verknüpfung mit den Druckertreibern (Vgl. Kapitel 6.5.2) eingerichtet werden.

6.5.2 Druckerfreigabe mit Druckertreiber verknüpfen

1. Starten Sie erneut den *Windows Explorer* und öffnen Sie die „*Netzwerkumgebung*“. Dort muss der „*Druckserver*“ („*Server*“) ausgewählt werden, auf dem die Druckerfreigabe angelegt wurde. In der oberen Menüleiste wird nach einem Klick auf *„Remotedrucker anzeigen“* eine Liste mit allen Druckerfreigaben angezeigt.

   Nun muss durch einen Klick mit der linken Maustaste ein Drucker ausgewählt werden, so dass dieser blau hinterlegt ist. (**Achtung**: Wurde der Drucker nicht durch einen Linksklick ausgewählt öffnet sich im Folgenden ein anderer Dialog). Einen Rechtsklick auf den Drucker ausführen und dann *“Eigenschaften“* auswählen

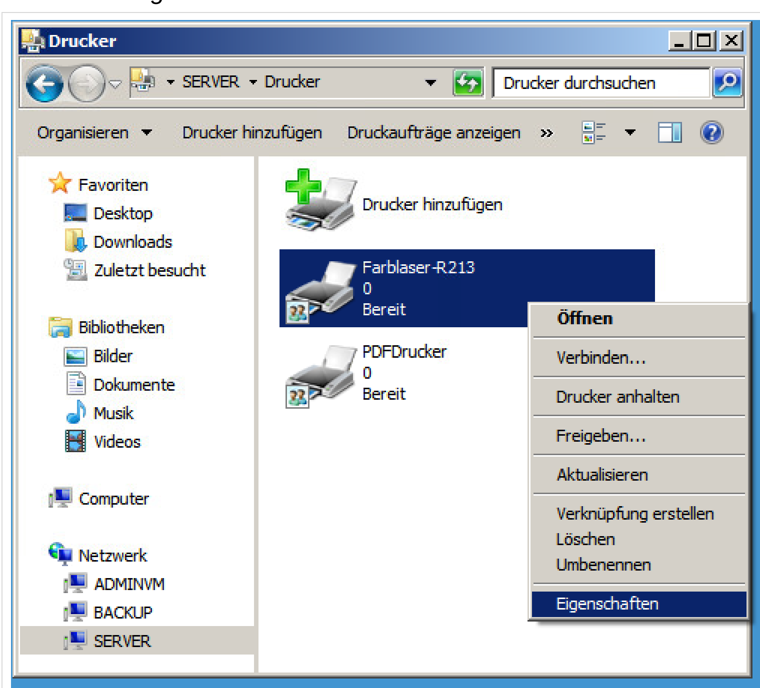


Abb. 103: Öffnen der Eigenschaften der Druckerfreigabe

2. Ist noch kein Druckertreiber installiert, wird die Fehlermeldung („*Der Druckertreiber "" ist nicht installiert…*“) angezeigt, die mit „*Nein*“ beantwortet werden muss.

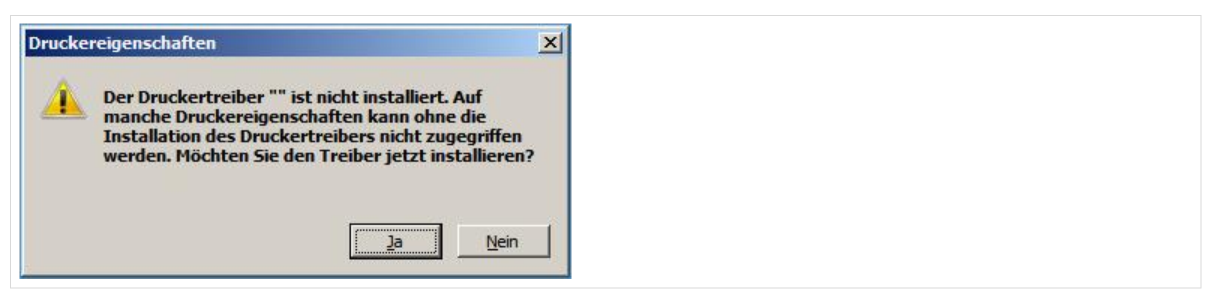


Abb. 104: Fehlermeldung bei fehlendem Druckertreiber

3. Nun muss im Reiter *„Erweitert"* unter *„Neuer Treiber"* der hochgeladene Treiber aus dem Dropdown-Menü ausgewählt werden. Anschließend muss auf *„Übernehmen"* geklickt werden. **Wichtig: Nicht auf „*OK*" klicken!**

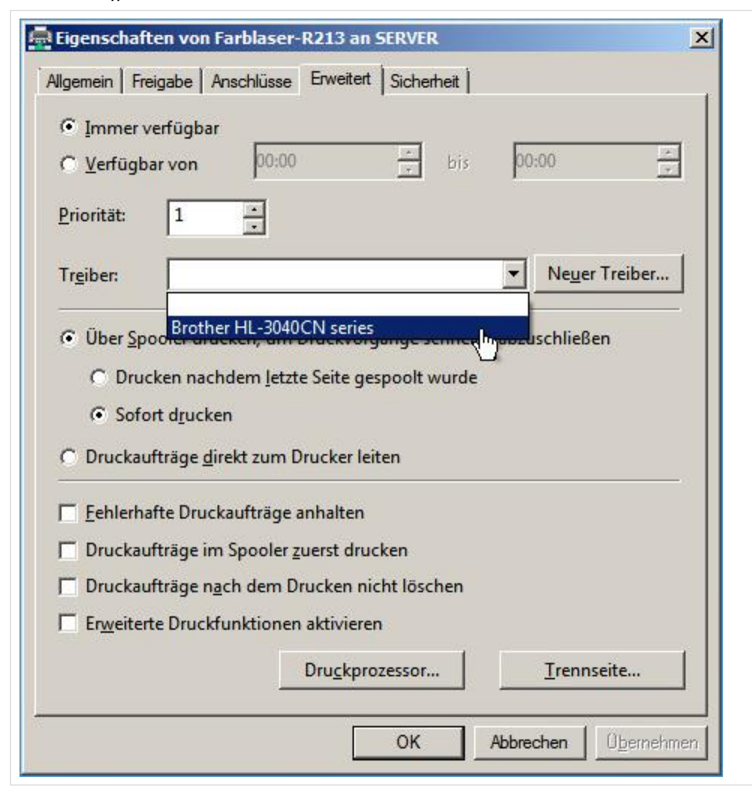


Abb. 105: Auswahl des neu hochgeladenen Treibers

Jetzt wird ein Dialog angezeigt, in dem gefragt wird, ob dem Drucker vertraut wird. Dies muss mit *„Treiber installieren"* bestätigt werden.



An diesem Punkt kann es zu einer Fehlermeldung kommen, die statt der Vertrauenswarnung erscheint.

Führen Sie die folgenden Schritte trotzdem durch. In der Regel funktioniert die Druckereinrichtung trotz der Fehlermeldung.

Wichtig: **Nun darf wieder nicht direkt auf „*OK*“ geklickt werden**, sondern es muss auf den Reiter *„Allgemein“* gewechselt werden. In dem Reiter muss weiterhin der alte Name der Druckerfreigabe angezeigt werden.

Es kann vorkommen, dass die Druckerfreigabe umbenannt wurde, damit ist sie dann nicht mehr mit der Freigabe verknüpft. Um Probleme, die dadurch auftreten, zu vermeiden, muss der Name des Druckers im Reiter *„Allgemein“* (das erste Eingabefeld, neben dem stilisierten Druckersymbol) immer pro forma auf den Namen der Druckerfreigabe geändert werden.

Hierbei ist der in der Druckerverwaltung der Schulkonsole (vgl. Tabelle Seite 100) eingetragene Name für den Drucker zu verwenden.



Abb. 106: Die Druckernamen müssen übereinstimmen

4. Anschließend auf *„Übernehmen“* und *„OK“* klicken. Nun werden die serverseitig hinterlegten Druckertreiber auf den Client heruntergeladen, sodass von dort aus z.B. direkt eine Testseite gedruckt werden kann.

6.6 Druckerzuordnung an Räume

Aufruf über Schulkonsole (als Administrator): Domäne | Gruppen

Die Zuordnung von Druckern an Räume geschieht über das Schulkonsolenmenü *„Domäne* | *Gruppen*“.

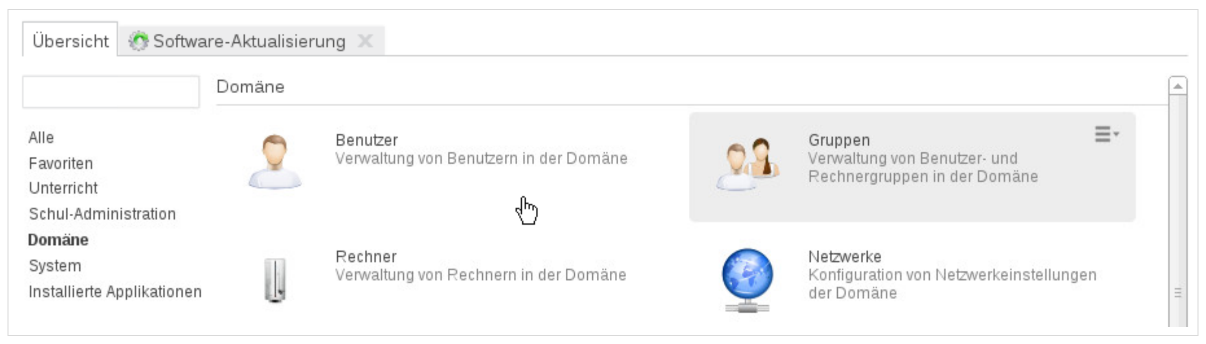


Abb. 107: Drucker werden über Gruppen an Räume zugewiesen

Wenn Sie dieses Modul öffnen, dann bekommen Sie alle Gruppen der *paedML Linux* angezeigt. Hierzu gehören Benutzergruppen, Klassen und Räume. Letztere benötigen wir, um einen Drucker einem Raum zuzuweisen.

Sie können die Anzeige auf Räume begrenzen, in dem Sie auf das Feld „*Erweiterte Optionen*“ klicken und im Dropdown-Menü „*Suche In:*“ den Container „*lokal.paedml-linux:/schule/groups/raeume*“ auswählen. Wenn Sie auf „Suche“ klicken, werden nur noch Computerräume angezeigt. Räume haben den Präfix „*schule-*“, zum Beispiel „*schule-r119*“.

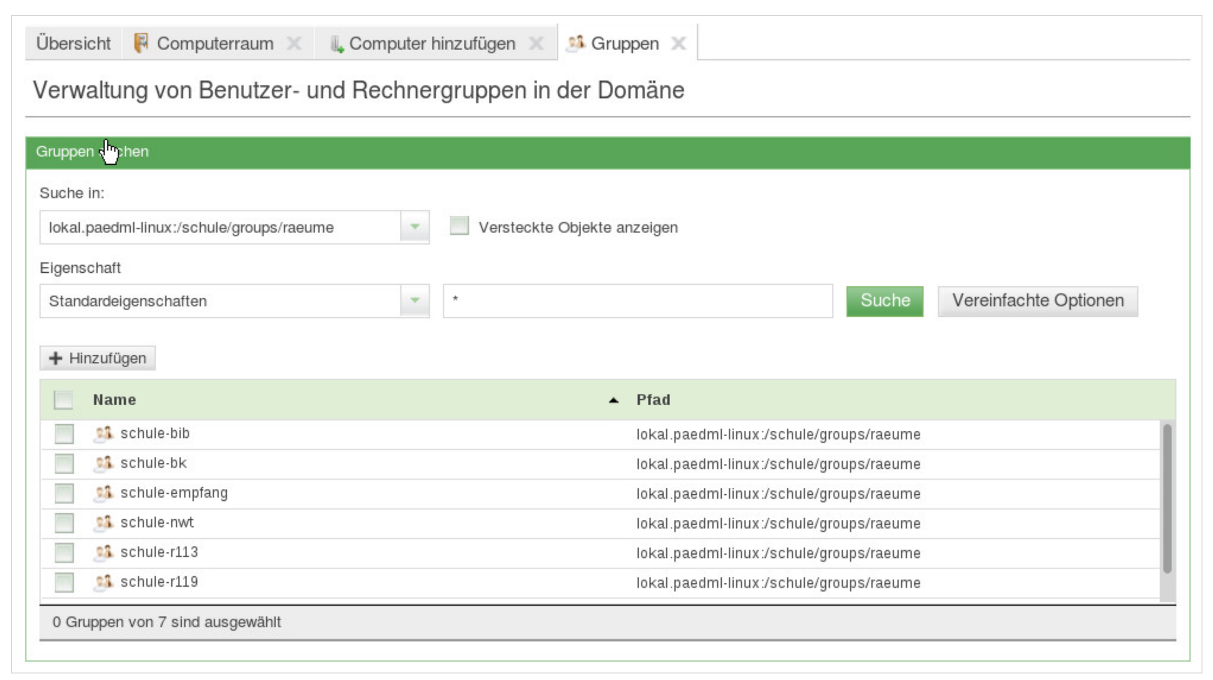


Abb. 108: Einschränken der Anzeige auf Computerräume

Anschließend können Sie den Raum auswählen, dem Sie den Drucker zuordnen wollen. Klicken Sie auf den Raum und navigieren Sie zum Reiter „*Druckerzuordnung*“. Im Drop-Down-enü „*Zugewiesene Drucker*“ können Sie einen Drucker auswählen und mit „*Änderungen speichern*“ dem Raum zuweisen.

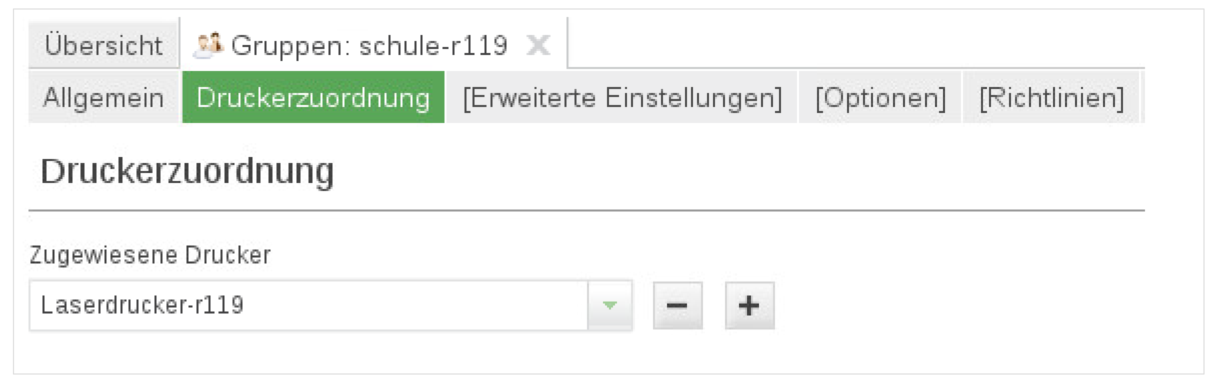


Abb. 109: Auswahl des Druckers

Der Drucker ist anschließend dem Raum zugeordnet. Beim Login der Benutzer wird der dem Raum zugeordnete Drucker auf dem Rechner eingerichtet und der Treiber wird installiert.

6.7 Manuelle Einrichtung des Druckertreibers am Client



Das im Folgenden beschriebene Verfahren funktioniert nur für einzelne Arbeitsplätze. Empfohlen wird ausdrücklich Drucker über die Schulkonsole (vgl. Kapitel 6.6, Seite 112) einzurichten.

Die in der *Schulkonsole* eingerichteten Druckerfreigaben können auf *Windows*-Systemen als Netzwerkdrucker hinzugefügt werden. Dies erfolgt unter *Windows* über die Systemsteuerung unter „*Drucker* | *Netzwerkdrucker hinzufügen*". Die Druckertreiber müssen beim ersten Zugriff eingerichtet werden. Wurden die Treiber serverseitig hinterlegt (siehe vorheriger Abschnitt), erfolgt die Zuweisung des Treibers automatisch.

Druckerfreigaben werden in der Regel mit den mitgelieferten *Windows*-Druckertreibern betrieben. Der Netzwerkdrucker kann auf *Windows*-Seite alternativ mit einem Standard-PostScript-Druckertreiber eingerichtet werden. Wenn auf einen Farbdrucker zugegriffen werden soll, sollte auf *Windows*-Seite ein Treiber für einen PostScript-fähigen Farbdrucker verwendet werden, z.B. *HP Color Laserjet 8550*.



Der Zugriff auf einen Drucker ist für einen regulären Benutzer nur möglich wenn dieser über lokale Rechte zur Treiberinstallation verfügt oder ein entsprechender Druckertreiber auf dem Druckserver hinterlegt wurde.

Ist dies nicht der Fall kann es zu einer *Windows*-Fehlermeldung kommen, die besagt, dass die Berechtigungen nicht ausreichen, um eine Verbindung mit dem Drucker herzustellen.

6.8 Erstellen von PDF-Dokumenten (für die Druckermoderation)



Das Konzept der Druckermoderation sieht vor, dass an Arbeitsplatzrechnern KEINE Hardwaredrucker eingerichtet sind.

Druckaufträge werden lediglich über den PDF-Drucker erstellt und müssen durch den unterrichtenden Lehrer freigegeben (bzw. ausgedruckt) werden.

Die Druckermoderation ist im Lehrerhandbuch beschrieben.

Durch das auf dem Server installierte Paket `univention-printserver-pdf` wird der Druckserver um den speziellen Druckertyp *cups-pdf* erweitert, der eingehende Druckaufträge in das PDF-Format umwandelt und für den jeweiligen Benutzer lesbar in ein Verzeichnis auf dem Druckserver ausgibt.

Im Auslieferungsstandard werden Druckaufträge nach */var/spool/cups-pdf/BENUTZERNAME* gedruckt, so dass der PDF-Drucker für jeden Benutzer ein eigenes Verzeichnis verwendet.

Anonym eingegangene Druckaufträge werden in das Verzeichnis */var/spool/cups-pdf* ausgegeben.

Der PDF-Drucker wird automatisch an jedem Client eingerichtet und steht jedem Benutzer zur Verfügung. Um eine PDF-Datei zu drucken, muss beim Druckauftrag einfach der „*PDF-Drucker am Server*" (\\server\PDFDrucker") ausgewählt werden. Die Druckausgabe wird in eine Textdatei umgeleitet.

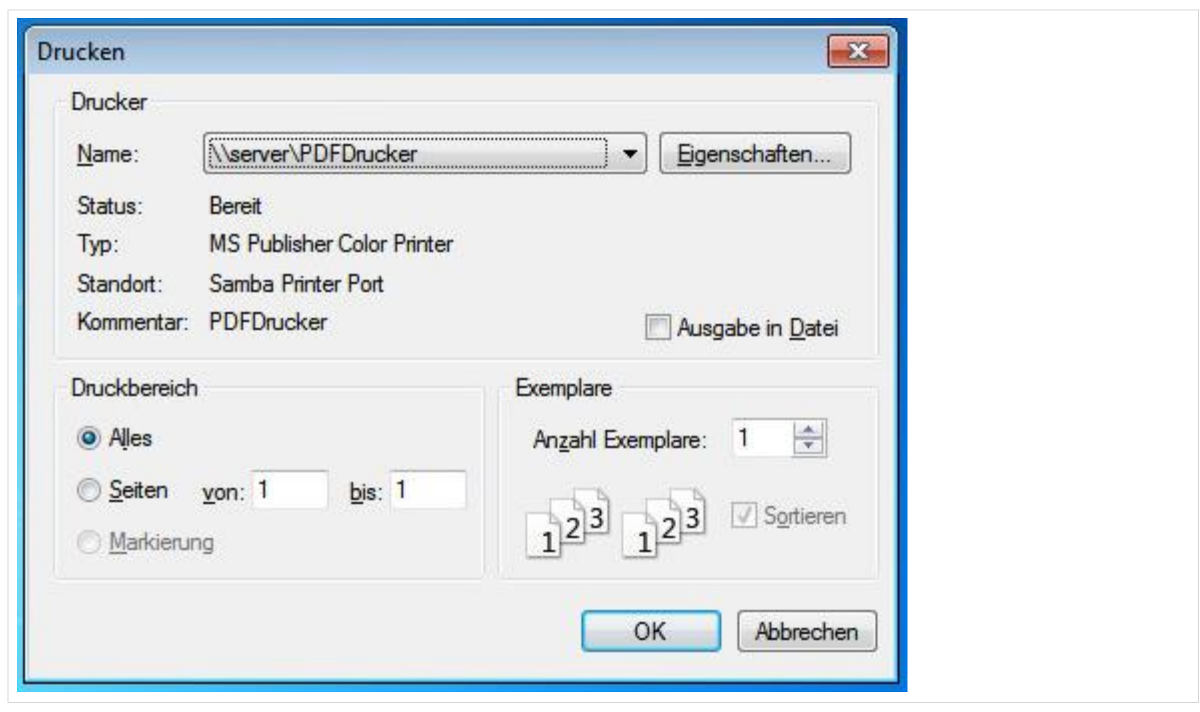


Abb. 110: Druckauftrag an den PDF-Drucker senden

Der Zugriff auf das „gedruckte“ Dokument geschieht über die Verknüpfung „*Eigene Shares/pdfPrinterShare*“, die jeder Benutzer auf dem Desktop hat. Der Zugriff ist erst dann möglich, wenn Druckaufträge in diesem Verzeichnis vorhanden sind.

Alternativ können Sie in der Netzwerkumgebung auf den Pfad *\\SERVER\pdfPrinterShare* navigieren. Dort befinden sich die „gedruckten“ PDF-Dateien.

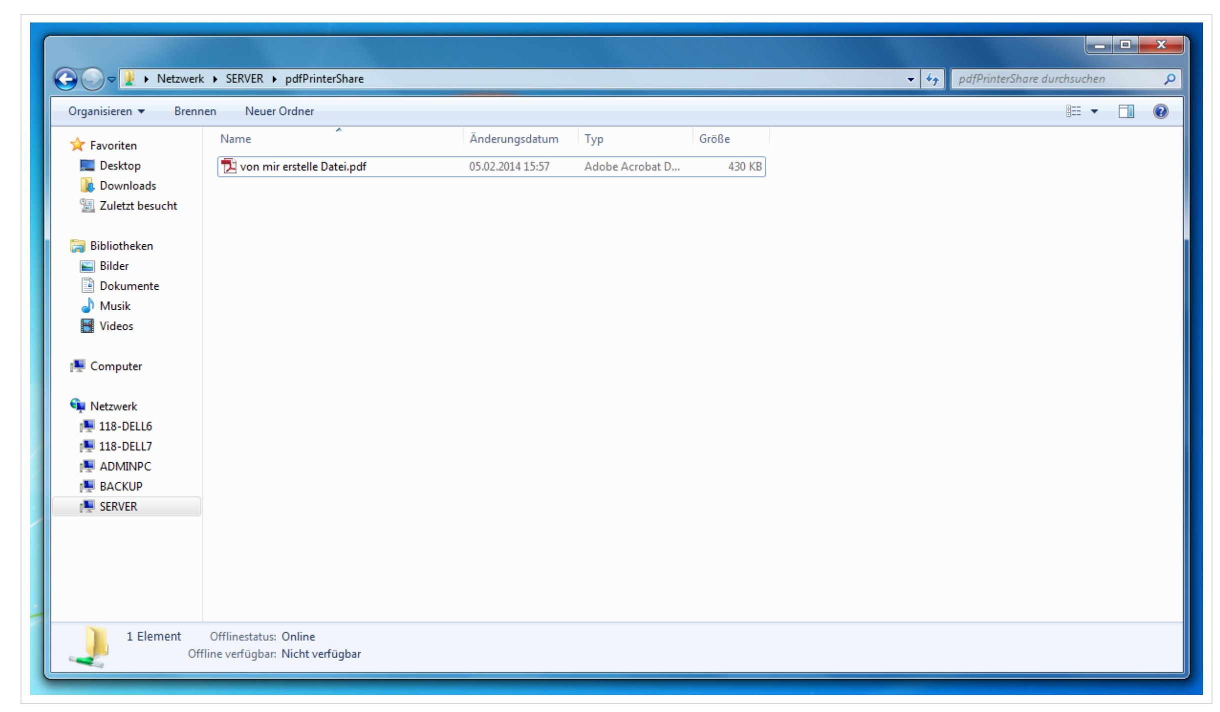


Abb. 111: \\Server\pdfPrinterShare - der Speicherort der PDF-Dateien.

7. Einrichtung der Arbeitsplatzrechner

Aufruf über Startseite https://server.paedml-linux.lokal | Reiter „Administration“ | Knopf: „OPSI *Windows*-Client Management“ oder

https://backup.paedml-linux.lokal:4447/configed oder

Aufruf über opsi-Anwendung, die lokal auf Rechnern installiert werden kann



Generell gilt, dass Rechner, die mit opsi verwaltet werden sollen, immer über PXE gebootet werden müssen.

Nur so bekommen die Rechner über das Netzwerk ein Signal gesendet, wenn opsi Aktionen wie die Installation von Betriebssystem, das Erstellen oder Wiederherstellen von Backups,… vorgesehen ist.



Bitte beachten Sie unbedingt die Hinweise zur Nomenklatur der *paedML Linux* im Anhang A, Seite 295.

Übersicht

- Im nächsten Unterkapitel bekommen Sie einen kurzen Einblick in die Mechanismen von *opsi*. Dabei werden einerseits kurz die Programmabläufe, andererseits die “*opsi*-Produkttypen“ (*Netboot*- und *Localboot-Produkte*) vorgestellt.
- Die Anmeldung an der *opsi*-Konsole wird in Kapitel 7.2 beschrieben.
- Im Anschluss (Kapitel 7.3, Seite 123) geben wir einen Überblick über die Benutzeroberfläche, den *opsi-configed* (*opsi configuration editor*).
- Kapitel 7.4 (S. 130 ff.) beschreibt, wie Sie die Installationsdateien für die Installation des Betriebssystems auf dem Server einspielen.
- Die Installation von *Windows* auf den Arbeitsplatzrechnern wird in Kapitel 7.5 (ab Seite 134) beschrieben.
- *opsi* bietet Ihnen die Möglichkeit, Hardwaretreiber auf die Arbeitsstationen zu verteilen (Kapitel 7.6 ab Seite 140), um die unterschiedlichen Hardwarekomponenten Ihres Schulnetzes zu unterstützen.
- Das folgende Unterkapitel 7.8 ab Seite 149 zeigt, wie Sie sich bei Bootproblemen, die hardwareseitig bedingt sind, helfen können.
- Es folgen die Beschreibung der Softwareinstallation (vgl. Kapitel 7.9) und
- Hinweise zu Programmpaketen, die für den Betrieb mit der *paedML Linux* notwendig sind (vgl. Kapitel 7.10, Seite 155).
- Im Anschluss folgen Hinweise zur Integration weiterer Softwarepakete (vgl. Kapitel 7.11 und 7.13, S. 155 ff.).
- Die Beschreibung über die Auswahl und gleichzeitige Installation mehrerer Rechner (z.B. eines Computerraumes) schließt das Kapitel ab (vgl. Kapitel 7.14 ab Seite 159).

7.1 Einführung in opsi

Das Clientmanagementsystem *opsi* („*open pc server integration*“) wird zur Verwaltung von *Windows*-Clients verwendet. Mit *opsi* können Sie das Betriebssystem ausrollen, Software verteilen und die Rechner des Schulnetzes mit Updates versorgen.



opsi ist ein umfangreiches Softwaremanagement-System, dessen gesamter Funktionsumfang in dieser Anleitung nicht abgebildet werden kann.

Wir beschreiben hier, die für den Betrieb der *paedML Linux* wesentlichen Features von *opsi*. Wenn Sie nähere Informationen zu *opsi* benötigen, dann nehmen Sie bitte Kontakt mit der Hotline auf.

Weitergehende Informationen zu *opsi* finden Sie auf der Webseite des Herstellers unter http://uib.de/de/opsi-dokumentation/dokumentationen.

opsi wird als „Gesamtpaket“ auf dem *paedML*-System „*OPSI-Server“* installiert. *opsi* besteht aus mehreren Komponenten, deren Zusammenspiel dafür sorgt, dass die Arbeitsplatzrechner mit Software versorgt werden:

5. Auf dem *opsi*-Server (Backup-Server) läuft eine *Datenbank*, in der gespeichert wird, welche Software auf einem Rechner installiert ist. In dieser Datenbank werden alle *opsi*-Aktionen protokolliert. Hier finden sich Einträge über erfolgte oder fehlgeschlagene Installationen. Pakete, die installiert werden sollen, werden mit einem entsprechenden Vermerk versehen.
6. Im sogenannten *opsi-Depot* (Verzeichnis /var/lib/opsi/depot) liegen alle Softwarekomponenten (*opsi-Produkte*), die installiert werden können (s. u.).
7. Ein listener-notifier-Mechanismus sorgt dafür, dass bei Bedarf die Software installiert wird.
    7.1. Auf dem Server läuft ein Webservice (*opsiconfd*), der die Informationen über neue Softwarepakete an die Clients übermittelt (notifier).
    7.2. Auf den Clients läuft ein Agent (*opsi-winst*), der beim Systemstart mit dem Betriebssystem gestartet wird und Befehle von *opsiconfd* entgegennimmt (listener).

    Wenn ein Paket zur Installation vorgemerkt ist, wir dieses auf den Client ausgespielt. Die Installation geschieht in der Regel beim Start der Maschine[34], kann über die *opsi*-Management-Konsole aber auch manuell gestartet werden.
8. Die Konfiguration der *opsi*-Datenbank geschieht über das Programm „*opsi-configed*“. Dieses kann an der Konsole des Backup-Servers mit *opsi*-Befehlen bedient werden. Angenehmer in der Bedienung ist die grafische opsi-Mangement-Konsole. *ospi-configed* kann als Paket auf den Clients installiert oder über einen Webbrowser ausgeführt werden.

[34] Hierbei wird – sofern der Rechner über PXE-Boot gestartet wird – eine Routine ausgeführt, über die Software vor dem Start des Betriebssystems verteilt wird.

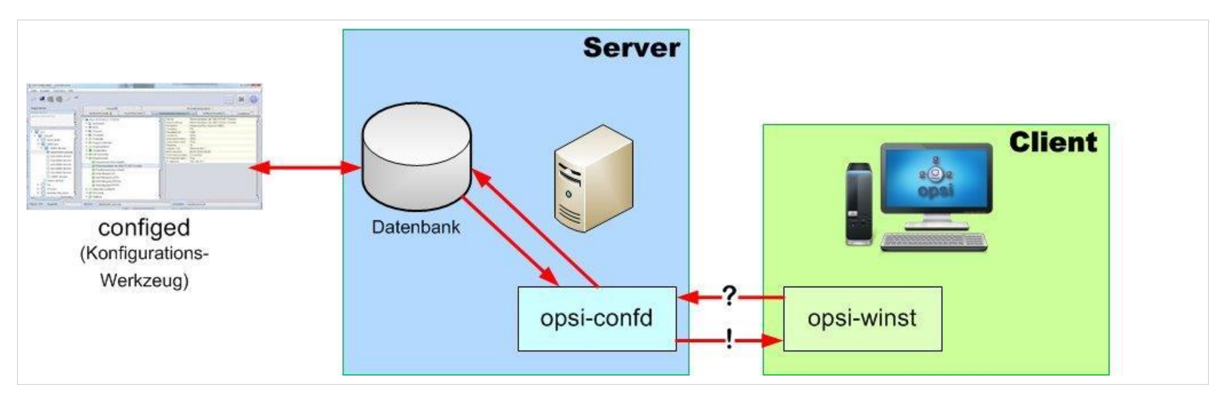


Abb. 112: schematische Darstellung von opsi

7.1.1 opsi-Produkte

In der Benutzeroberfläche von *opsi* werden alle installierbaren Softwarekomponenten als *opsi-Produkte* bezeichnet. *opsi*-Produkte werden unterteilt in *Netboot-Produkte* und *Localboot-Produkte*.

1. *Netboot-Produkte* sind Routinen, die beim Starten eines Rechners über PXE ausgeführt werden. Hierzu zählt die Installation von *Windows* sowie die Erstellung und Wiederherstellung von lokalen Rechnerabbildern.
2. *Localboot-Produkte* sind vor allem Anwendungen, die auf den Rechnern installiert werden. Hierzu zählen Officepakete, Internetprogramme und andere Anwendungen. Daneben finden sich in diesem Bereich *Microsoft „Hotfixes*" für *Windows* und *Microsoft Office* sowie Skripte für Aktionen wie den Domänenbeitritt oder das Herunterfahren der Rechner. Diese, sind unter dem Reiter Produktkonfi-guration zu finden.

opsi verwaltet seine Pakete in einem sogenannten *opsi-Depot*. Der Speicherort auf dem *opsi*-Server ist */var/lib/opsi/depot*. Dieser Ort ist auch als *Windows*-Freigabe aufrufbar. Daten für das opsi-Depot müssen über die opsi-Konsole (opsi-configed) eingespielt werden.

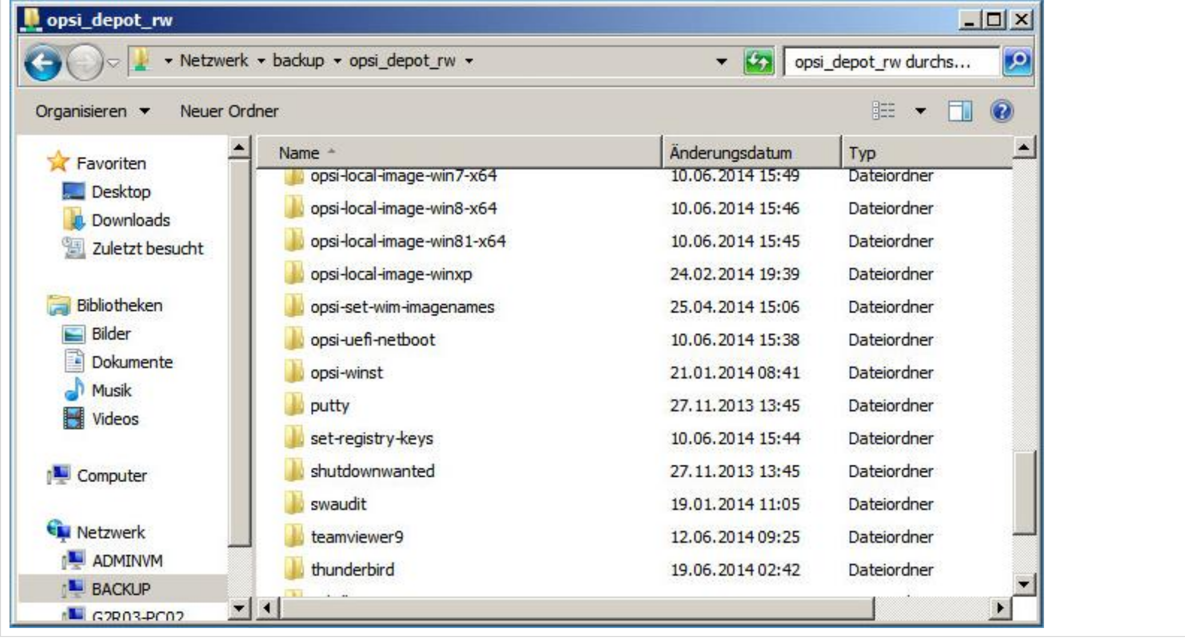


Abb. 113: *Einblick in das opsi-Depot via* Windows-*Explorer*

In dieses Verzeichnis werden alle auf *Windows*rechnern zu installierenden Softwarepakete abgelegt. Das Einspielen von *opsi*-Paketen auf dem *Backup-Server* wird im Kapitel 7.9 auf Seite 153 beschrieben.

7.2 Start von opsi-configed



Damit Sie *opsi* auf einem Rechner bedienen können, benötigen Sie ein aktuelles *Java Runtime Environment*[35]. Sie können *opsi* mit jedem Betriebssystem im Browser (Java installiert) aufrufen. *Java* gibt es als *opsi*-Paket, das auf die Rechner verteilt werden kann.

7.2.1 Lokaler Start

Das *opsi*-Paket *opsi-configed* kann auf jedem Rechner im Netzwerk installiert werden. Das Programm ist Bestandteil der Standardinstallation der virtuellen Maschine *AdminVM*.

Wenn das Programm installiert wurde, dann können Sie es über eine Verknüpfung im Startmenü öffnen.

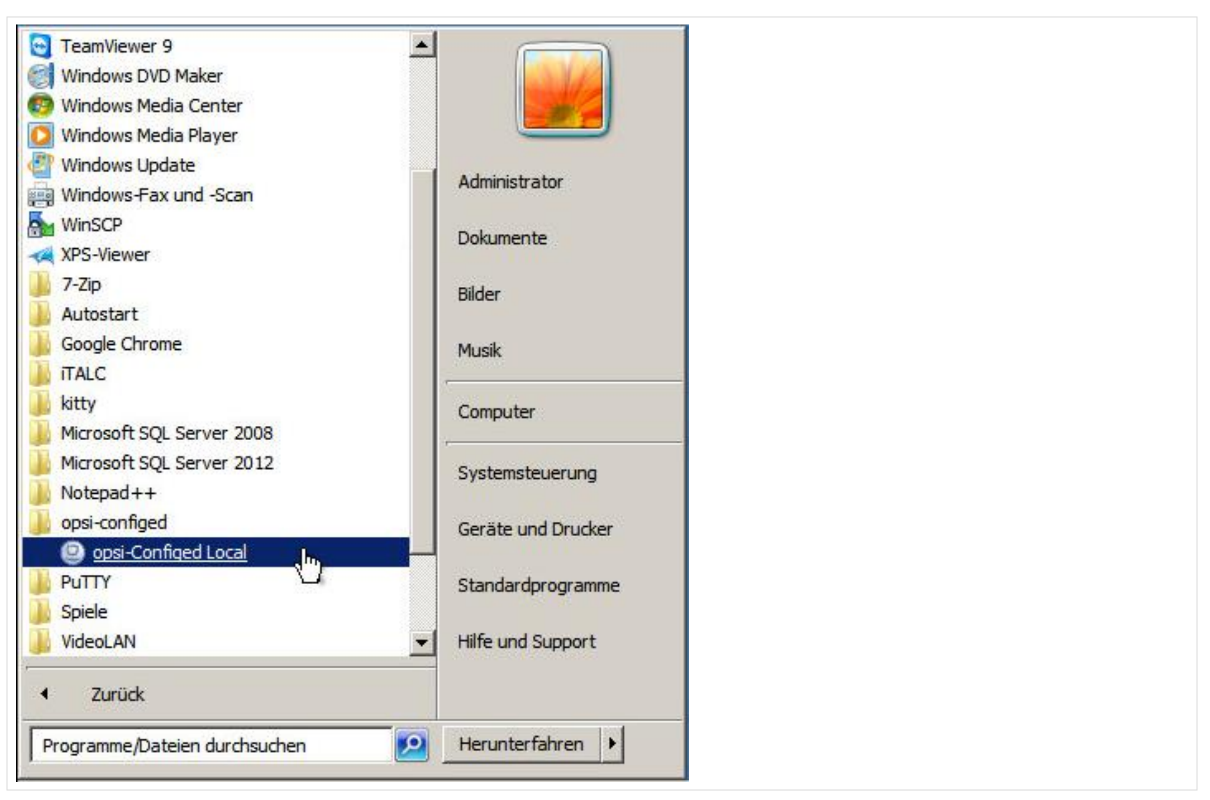


Abb. 114: Aufruf des lokalen opsi-Konfigurationspgrogrammes

Wenn Sie das Programm ausführen, werden Sie nach Benutzernamen und Passwort gefragt. Geben Sie hier die Zugangsdaten für den Benutzer *Administrator* (mit großem A) ein. Wenn Sie sich mit dem

[35] http://www.java.com/de/download/

„falschen“ „administrator“ anmelden, erhalten Sie – neben einer Fehlermeldung – eine leere *opsi*-Konsole, in der keine Clients ausgewählt werden können.

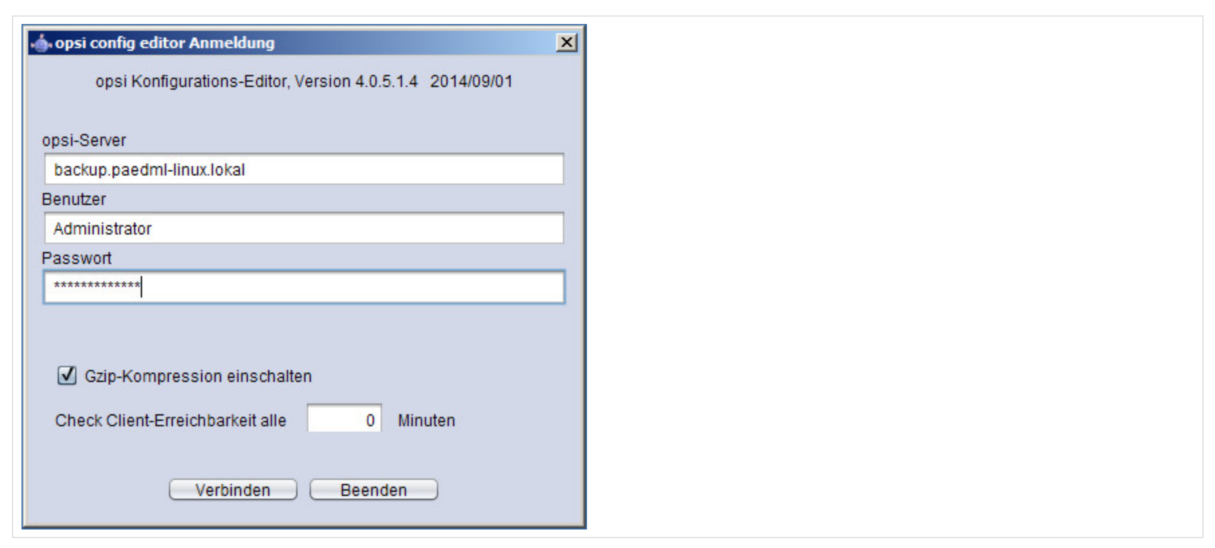


Abb. 115: Anmeldung an der opsi-Konsole als Domänen-Administrator

7.2.2 Anmeldung an opsi via Webzugriff

opsi-configed kann aber auch ohne lokale Installation über einen Webbrowser gestartet werden.



Der Webzugriff sollte nur dann genutzt werden, wenn keine lokale *opsi-configed*-Installation vorhanden ist. Das auf den Rechnern installierte opsi-Programmpaket ist unter Umständen aktueller, wie die Web-Version.

Aufgrund einer Anpassung in der Sicherheit von *Java* ist der Zugriff von einem *Windows*-Rechner auf opsi blockiert.Um dennoch auf opsi zugreifen zu können, muss eine Ausnahme für das Ausführen von *Java* Anwendungen des Backup-Servers in der *Java*-Konfiguration eingetragen werden.

Um die *Java*-Konfiguration anzupassen, öffnen Sie „*Start* | *Programme* | *Java* | *Configure Java*“. (Alternativ über die *Systemsteuerung*, Menüpunkt „*Java*“)

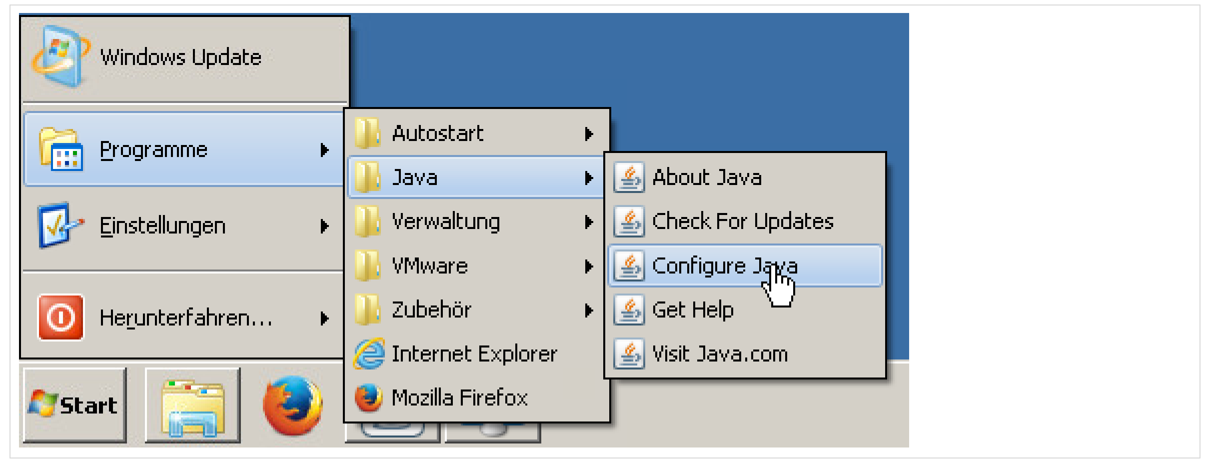


Abb. 116: Öffnen der Java-Konfiguration

Im sich nun öffnenden Fenster „*Java-Control-Panel*“ navigieren Sie auf den Reiter „*Sicherheit*“. Klicken Sie auf „*Sitelist bearbeiten…*“, um den Backup-Server einzutragen. Es öffnet sich ein neues Fenster.

Klicken Sie auf „*Hinzufügen*“, um eine Ausnahme zu erstellen. Tragen Sie „*https://backup.paedml-linux.lokal:4447/configed*“ in das entsprechende Feld ein. Und bestätigen Sie den Eintrag mit „*OK*“.

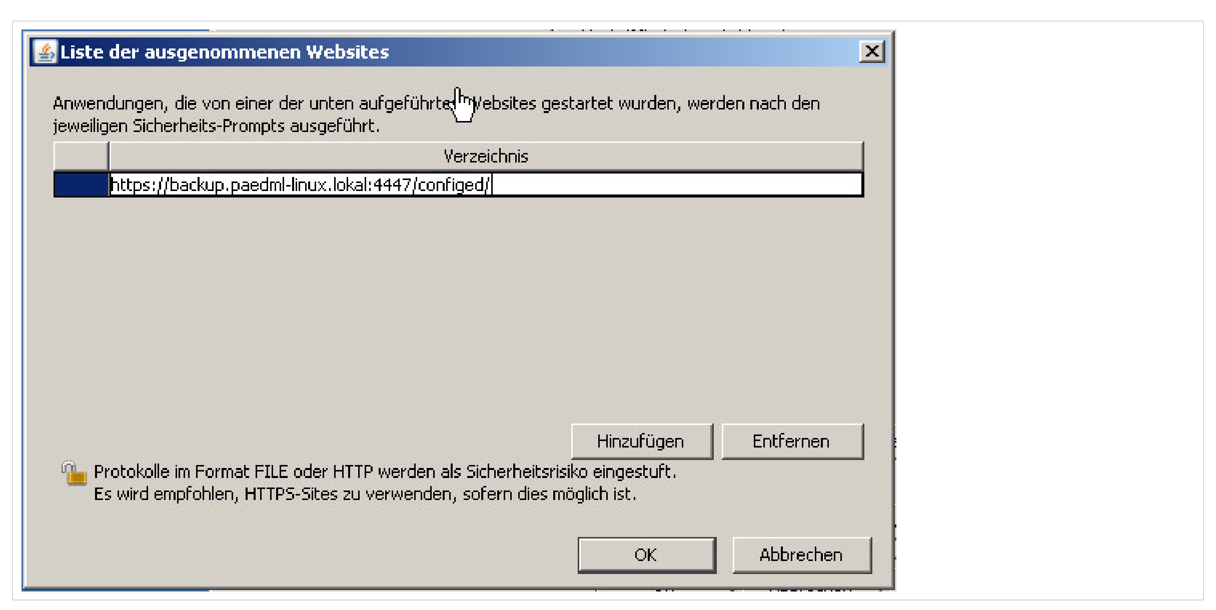


Abb. 117: Hinzufügen einer Ausnahme für Java

Schließen Sie das „*Java-Control-Panel*“, in dem Sie nochmals „*OK*“ drücken. Die Ausnahme ist nun eingetragen und aktiv.

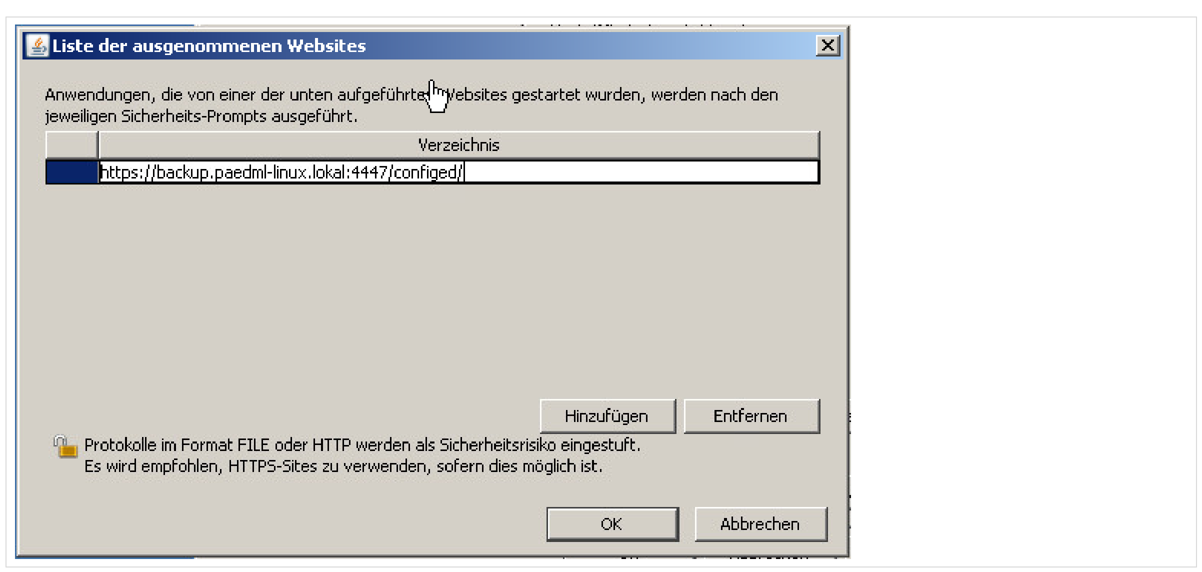


Abb. 118: Ausnahme eingetragen

Wenn Sie *opsi* aufrufen, müssen Sie zunächst Sicherheitswarnungen quittieren. Die Meldungen können variieren – abhängig von Ihrer *Java*-Version.

Die erste Sicherheitswarnung bezieht sich auf die Vertrauenswürdigkeit der Anwendung. Klicken Sie auf „*Weiter*“.

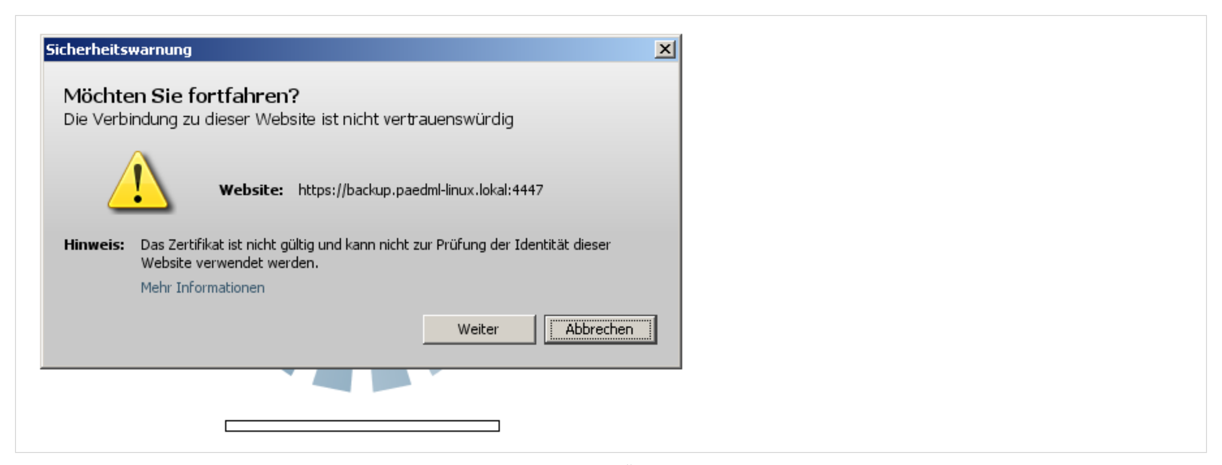


Abb. 119: Zertifikatsprüfung durch den Browser. Mit „Weiter“ quittieren

Akzeptieren Sie im zweiten Dialog das „Risiko“, die Anwendung auszuführen. Setzen Sie hierfür das entsprechende Häkchen und klicken sie auf „*Ausführen*“.

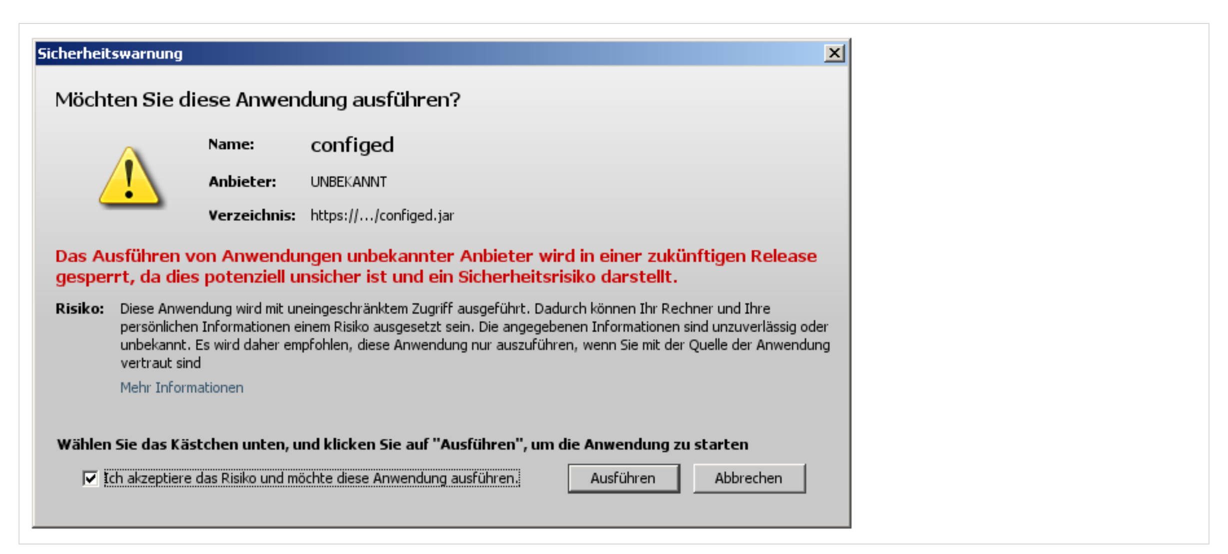


Abb. 120: Warnungsmeldung vor der Ausführung von Java-Programmcode von unbekanntem Anbieter

Nun müssen Sie sich mit Ihrem Administratorkonto (**Administrator mit großem A!**) und dem zugehörigen Kennwort an *opsi* anmelden.



Abb. 121: Anmeldung an der opsi-Oberfläche als Administrator der Domäne

7.3 Die Benutzeroberfläche



Wir raten dringend davon ab, nicht von uns dokumentierte Änderungen im *opsi-config editor*[36] vorzunehmen, da dies zu Problemen bei der Synchronisation mit dem paedML Server führen kann.

Sie sollten insbesondere keine Rechner über opsi anlegen oder angelegte Rechnerobjekte mit Hilfe von opsi ändern (zum Beispiel umbenennen von Clients).

Wir wollen Ihnen hier einen Überblick über die im Schulalltag wichtigsten Funktionen von *opsi* geben, wobei für die Verwaltung der Schulrechner nur ein Teil der *opsi*-Bausteine Relevanz hat. Die hier benannten *opsi*-Elemente haben wir in der Vorstellung der *opsi*-Benutzermaske mit Symbolen gekennzeichnet:

- ❋ - Diese Funktion ist wichtig für die Arbeit im Schulnetz.
- ★ - Ein „nice to have feature“. Das Modul unterstützt Sie bei der Arbeit, muss aber nicht zwangsweise genutzt werden.
- 💣 - Die Benutzung dieser Funktion führt mit hoher Wahrscheinlichkeit zu Problemen. Bitte nicht benutzen. Dieses Symbol kennzeichnet ferner Module, die nicht im Standardlieferumfang der *paedML Linux* enthalten sind (z.B. das Modul „Lizenzverwaltung“).

Die Benutzeroberfläche – der *opsi config editor* – teilt sich in sechs Bereiche auf (s. folgender Screenshot).

1. Die Menüleiste,
2. acht Knöpfe links oben,
3. sechs weitere Knöpfe rechts oben,
4. das Auswahlfenster, in dem Clients und Gruppen für die Konfiguration ausgewählt werden können,
5. das in verschiedene Reiter unterteilte Hauptfenster und
6. ein dynamischer Bereich, der, je nach selektiertem Modul im Hauptfenster mit Inhalt versorgt wird.

[36] In dieser Anleitung finden die Begriffe „opsi config editor“ und „opsi-Konsole“ für die Benennung der opsi-Benutzermaske Anwendung.

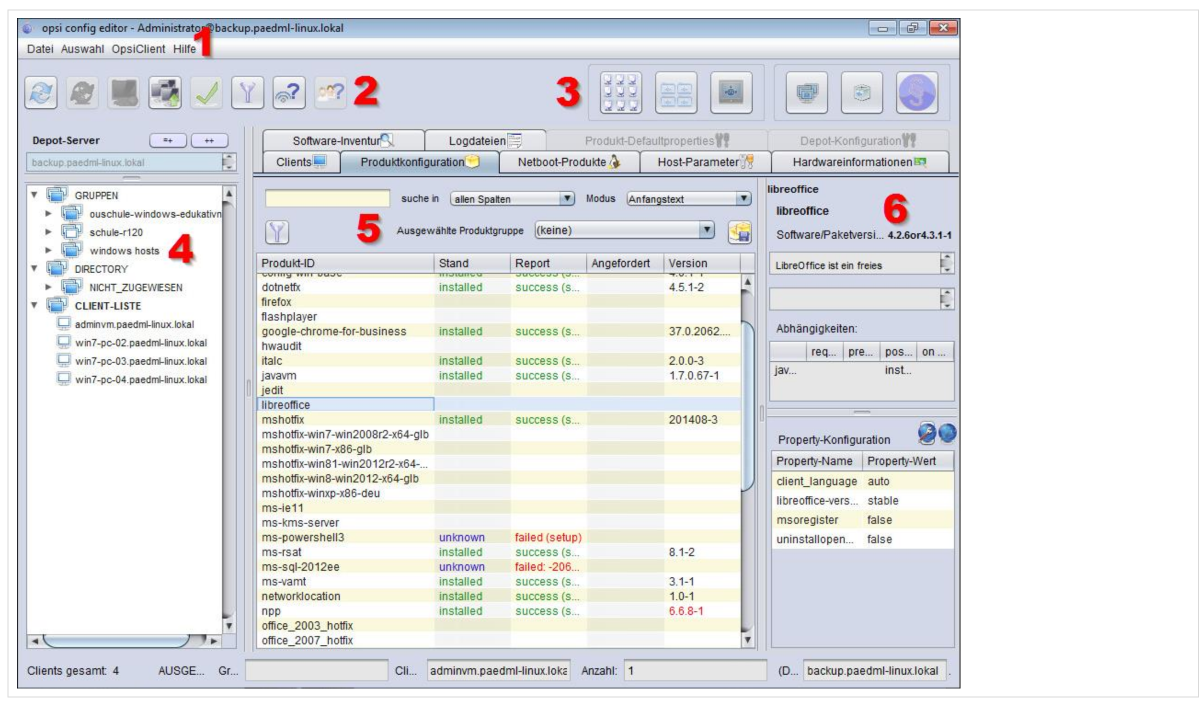


Abb. 122: Übersicht über den opsi config editor

Da wir hier in diesem Kapitel immer wieder auf die Übersicht der *opsi*-Konsole Bezug nehmen, finden Sie die Übersicht über die *opsi*-Konsole nochmals im Anhang. Sie können sich die Grafik für die Arbeit mit diesem Kapitel ausdrucken. Dadurch finden Sie sich hoffentlich schneller zurecht, wenn beispielsweise von der Rechnerliste (4) oder dem Hauptfenster (5) die Rede ist.

---

1. Die *Menüleiste*

Hinter der Menüleiste verbergen sich verschiedene Einträge, die größtenteils auch in der Hauptmaske abgebildet werden.

Datei Auswahl OpsiClient Hilfe

Abb. 123: Die Menüleiste von opsi

1.1. Unter „*Datei*“ befinden sich die folgenden Menüeinträge:

1.1.1. ✱ „*Speichern der Konfiguration*“

1.1.2. ✱ „*Alle Daten neu laden*“

1.1.3. ★ „*International*“ – hier können Sie die Sprache der Oberfläche auswählen.

1.1.4. ★ „*Beenden*“ – hierüber kann das Fenster geschlossen werden.

1.2. Unter „*Auswahl*“ finden Sie:

1.2.1. ★ „*Freie Anfrage*“ – öffnet ein neues Fenster, in dem Sie Rechner nach Eigenschaften suchen und auswählen können.

1.2.2. ★ „*Gespeicherte Anfragen*“ – "Freie Anfragen“ können gespeichert und wieder aufgerufen werden.

1.2.3. ★ „*Nicht aktuelles Produkt…*" – mit diesem Menüpunkt können Sie Rechner anzeigen lassen, bei denen ein ausgewähltes Programmpaket installiert ist, aber nicht in der aktuell verfügbaren Version vorliegt. Die Anzeige der betroffenen Rechner erfolgt im Reiter „*Clients*" im Hauptfenster.

1.2.4. ★ „*Fehlgeschlagene Aktionen bei Produkt…*" – …" – mit diesem Menüpunkt können Sie Programmepakete anzeigen lassen, die nicht vollständig installiert wurden. Die Anzeige der betroffenen Rechner erfolgt im Reiter „*Clients*" im Hauptfenster.★ „*Fehlgeschlagene Aktionen*" – zeigt an, welche Aktionen *opsi* nicht durchgeführt hat. Die Anzeige kann zeitlich eingegrenzt werden. Es werden hier, sowie beim vorigen Punkt nur Ergebnisse angezeigt, wenn Fehler in der Konfiguration der Rechner vorliegen. Die Anzeige der betroffenen Rechner erfolgt im Reiter „*Clients*" im Hauptfenster.

1.2.5. ★ „*Nur die ausgewählten Clients anzeigen*" – blendet alle Rechner aus, die nicht der Auswahl entsprechen.

1.3. Im Menü „*Opsi-Client*" sind verschiedene Menüpunkte, die das Verhalten von Rechnern steuern.

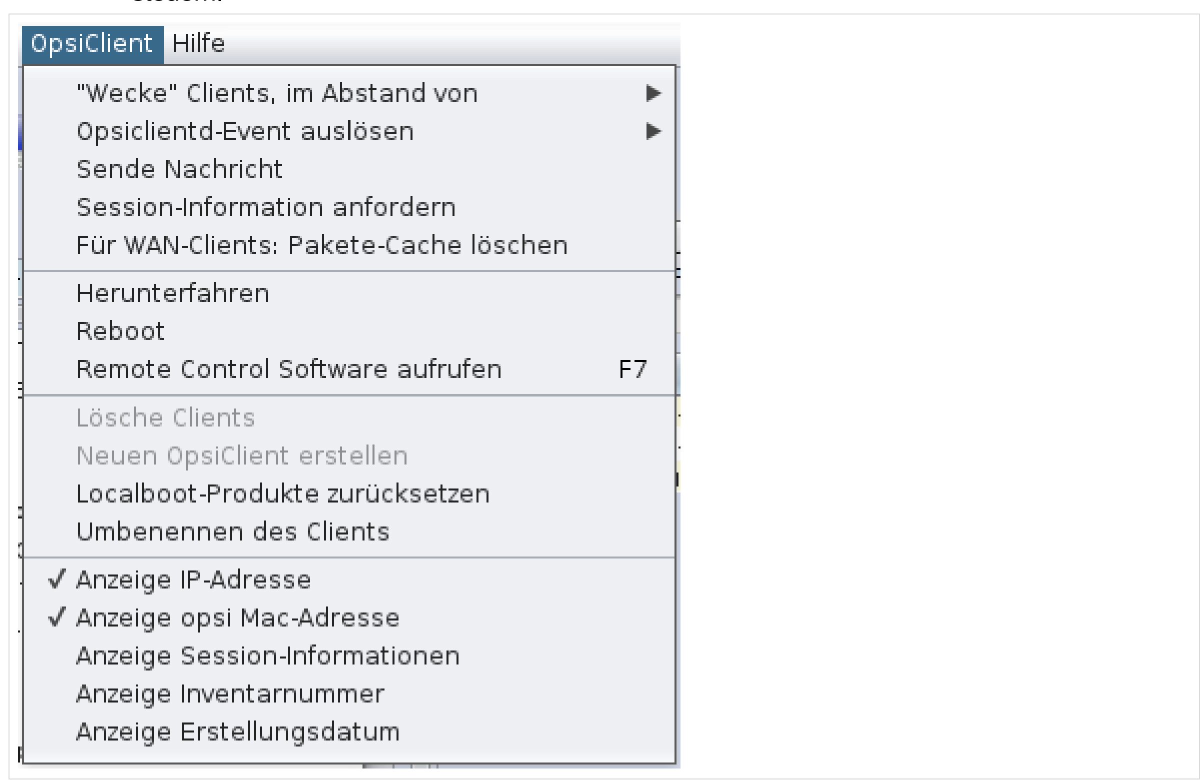


Abb. 124: Der Menüeintrag „OpsiClient"

1.3.1. ❋ „*Wecke Clients im Abstand von*" – hier können Sie einen Zeitraum festlegen, der ausgewertet wird, wenn markierte Rechner zeitgleich (0 Sekunden) oder zeitversetzt geweckt werden sollen.

1.3.2. ❋ „*opsiclientd-Event auslösen*" – Hinter diesem Menüeintrag finden Sie einen Eintrag „*on_demand*", mit dem Sie Änderungen sofort (bzw. beim nächsten Systemstart) an Rechner ausspielen können.

1.3.3. ✱ „*Sende Nachricht*“ – Hiermit können Sie Benutzern von selektierten Rechnern eine Nachricht auf den Monitor schicken. Dadurch können Anwender beispielsweise über das Ausspielen von Software informiert werden.

1.3.4. ✱ „*Session-Information anfordern*“ – Hiermit können Sie überprüfen, welche Benutzer an Clients angemeldet sind (Anzeige im Hauptfenster | Reiter „*Clients*“).

1.3.5. 💣 „*Für WAN-Clients: Pakete-Cache löschen*“ – Ohne Funktion in der paedML

1.3.6. ✱ „*Herunterfahren*“ – Hier können Sie – nach Bestätigung eines Dialogfensters – ausgewählte Clients herunterfahren.

1.3.7. ✱ „*Reboot*“ – Hier können Sie – nach Bestätigung eines Dialogfensters – ausgewählte Clients neu starten.

1.3.8. ★ „*Remote Control Software aufrufen*“ – hier können die ausgewählten Clients gepingt werden.

1.3.9. 💣 „*Lösche Clients*“ – **Deaktiviert.**

1.3.10. 💣 „*Neuen OpsiClient erstellen*“ – **Deaktiviert.**

1.3.11. ★ *„Localboot-Produkte zurücksetzen“* – löscht alle Einträge, die für einen Client in der Produktkonfiguration (Localboot-, nicht Netzboot-Produkte!) hinterlegt sind. Also die Informationen darüber, welche Software in welcher Version installiert ist. **Dieser Schritt ist notwendig, bevor ein Client neu installiert wird.**

1.3.12. 💣 „*Umbenennen des Clients*“ – **Nicht Benutzen!**

1.3.13. ★ „*Anzeige* …“ – Der untere Bereich dieses Menüs ermöglicht es Ihnen die Anzeige der Rechnerinformationen im Reiter „*Clients*“ des Hauptfensters (5) anzupassen. Sie können mit diesem Abschnitt Spalten ein- oder ausblenden.

1.4. ★ Der Menüeintrag „*Hilfe*“ verbirgt Verweise zu Unterstützungsangeboten rund um opsi. Hier können Sie außerdem Informationen rund um die opsi-Installation einsehen.

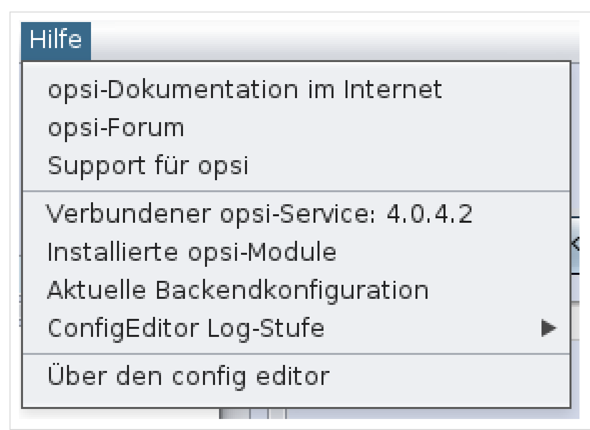


Abb. 125: Der Menüeintrag „Hilfe“

1.4.1. ★ Für die Fehlersuche relevant und daher hier gesondert erwähnt ist der Menüeintrag „*ConfigEditor Log-Stufe*“. Hier können Sie festlegen, welche Meldungen in die Log-Dateien geschrieben werden sollen („*Log-Level*“).

Unter der Menüleiste finden Sie verschiedene Symbole, die im Folgenden erklärt werden. Für alle Symbole des oberen Bereichs der opsi-Konfigurationsseite gibt es eine Beschreibung, die Sie angezeigt bekommen, wenn Sie mit dem Mauszeiger über dem jeweiligen Symbol verweilen.

2. Die *Symbole links oben* bieten einen Schnellzugriff auf Menüpunkte

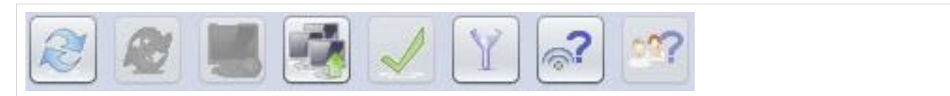


Abb. 126: Detail opsi config editor

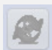
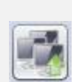
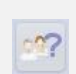
Symbol	Beschreibung
	❋ Mit dem ersten Symbol können Sie die Daten von opsi neu laden.
	💣 Die ausgegrauten Pfeile des nächsten Symbols sind nur aktiv, wenn die Lizenzverwaltung von opsi aktiviert ist. Hiermit können die Lizenzverwaltungsdaten neu eingelesen werden.
	💣 Der blaue Monitor fügt neue Rechner zu opsi hinzu. **Achtung! Diese Funktion darf nicht verwendet werden, wenn die Rechner mit der paedML Linux verwaltet werden. Das Symbol ist daher inaktiv.**
	✶ Mit dem nächsten Knopf können Sie eine Auswahl definieren. Ein Klick auf das Symbol öffnet ein neues Fenster, das Sie dafür nutzen, Rechner mit bestimmten Eigenschaften anzeigen zu lassen. Sie können Computer aus dem Schulnetz nach „*Host-Eigenschaften*“ (zum Beispiel IP-Adresse, Name („ID“), …) „*opsi Produkt-Eigenschaften*“ anzeigen lassen. Sie können aus einer großen Kriterienliste wählen, nach welchen Hardwareeigenschaften eine Auswahl von Rechnern angezeigt werden soll.
	❋ Das fünfte Symbol der Liste ist ein grüner Haken, der rot wird, wenn Sie Änderungen an der Konfiguration von Rechnern vorgenommen haben, die noch nicht gespeichert wurden. Um Änderungen zu speichern, muss der rote Haken angeklickt werden.
	✶ Der blaue Trichter ermöglicht es Ihnen, aus der Liste der Clients die nicht selektierten auszublenden und nur ausgewählte Clients zu zeigen.
	❋ Das nächste Symbol können Sie nutzen, um zu überprüfen, welche Rechner mit opsi verbunden sind.
	✶ Das letzte Symbol dieser Leiste bietet die Möglichkeit, im Hauptfenster (5) im Reiter “*Clients*“ eine „*Abfrage der Session-Informationen von allen Clients*“ anzeigen zu lassen. Um diese Informationen einsehen zu können, müssen Sie in der Menüleiste (1) im Menü „*Opsi-Client*“ den Punkt „Anzeige Session-Informationen“ aktivieren.

Tabelle 16: Symbole der opsi-Konsole

3. Einige der *Symbole rechts oben* helfen Ihnen bei der Navigation. Die Auswahl einzelner *opsi-*Komponenten (zum Beispiel das dritte Symbol „*Host-Parameter*“) ändern die Auswahlmöglichkeiten im Hauptfenster, die Sie mit hier beschriebenen Knöpfen wieder herstellen können.



Abb. 127: Detail opsi config editor

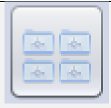
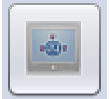
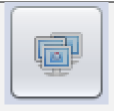
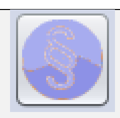
Symbol	Beschreibung
	★ Das erste Symbol auf der rechten Seite bringt Sie direkt in die Clientansicht („Clientkonfiguration“) des Hauptfensters (5).
	Über das nächste Symbol gelangen Sie zu den „Depoteigenschaften“. Hier dürfen keine Werte verändert werden!
	Das Monitorsymbol mit dem opsi-Logo führt zur „Server -Konfiguration“ und öffnet den besonderen Reiter „Host-Parameter“ im Hauptfenster (5). Mit diesem Knopf können Sie globale Parameter für die Clients einstellen. Hier bitte nichts ohne Rücksprache mit der Hotline ändern.
	★ „Gruppenbezogene Aktionen“ können über das nächste Symbol ausgeführt werden.
	✱ Die „Produktverwaltung“, also die Verwaltung von opsi-Paketen verbirgt sich hinter Symbol Nummer fünf. Hier können Sie opsi-Netboot-Produkte einspielen und Installations-dateien von *Windows* vervollständigen.
	Die Verwaltung von „Lizenzen“ verbirgt sich hinter dem letzten Symbol. Dieses Modul ist nicht aktiv. Mehr Informationen erhalten Sie über einen Klick auf den Knopf.

Tabelle 17: weitere Symbole der opsi-Konsole

4. ✱ Im weißen Fenster, der *Rechnerliste* auf der linken Seite, sehen Sie alle über die Schulkonsole aufgenommenen Rechner des Rechner Typs „*Windows-System“*.

   Sie können einzelne Rechner („*CLIENT-LISTE*“) oder „*GRUPPEN*“ (entspricht Computerräumen) auswählen. Die Auswahl von Gruppen wird in Kapitel 7.14 ab Seite 159 beschrieben. Mit Hilfe der Strg-Taste können Sie mehrere Objekte einzeln markieren (Strg gedrückt halten und mit der Maus

Clients hinzu- oder abwählen). Die Shift-Taste ermöglicht es Ihnen, größere Bereiche zwischen zwei Objekten hinzuzufügen oder abzuwählen. Ausgewählte Rechner werden markiert und in der Hauptseite (Punkt 5) im Reiter „*Clients*“ angezeigt.

Der Eintrag bei „*Depot-Server*“ zeigt den Namen des paedML-Servers, auf dem das opsi-Depot installiert ist.

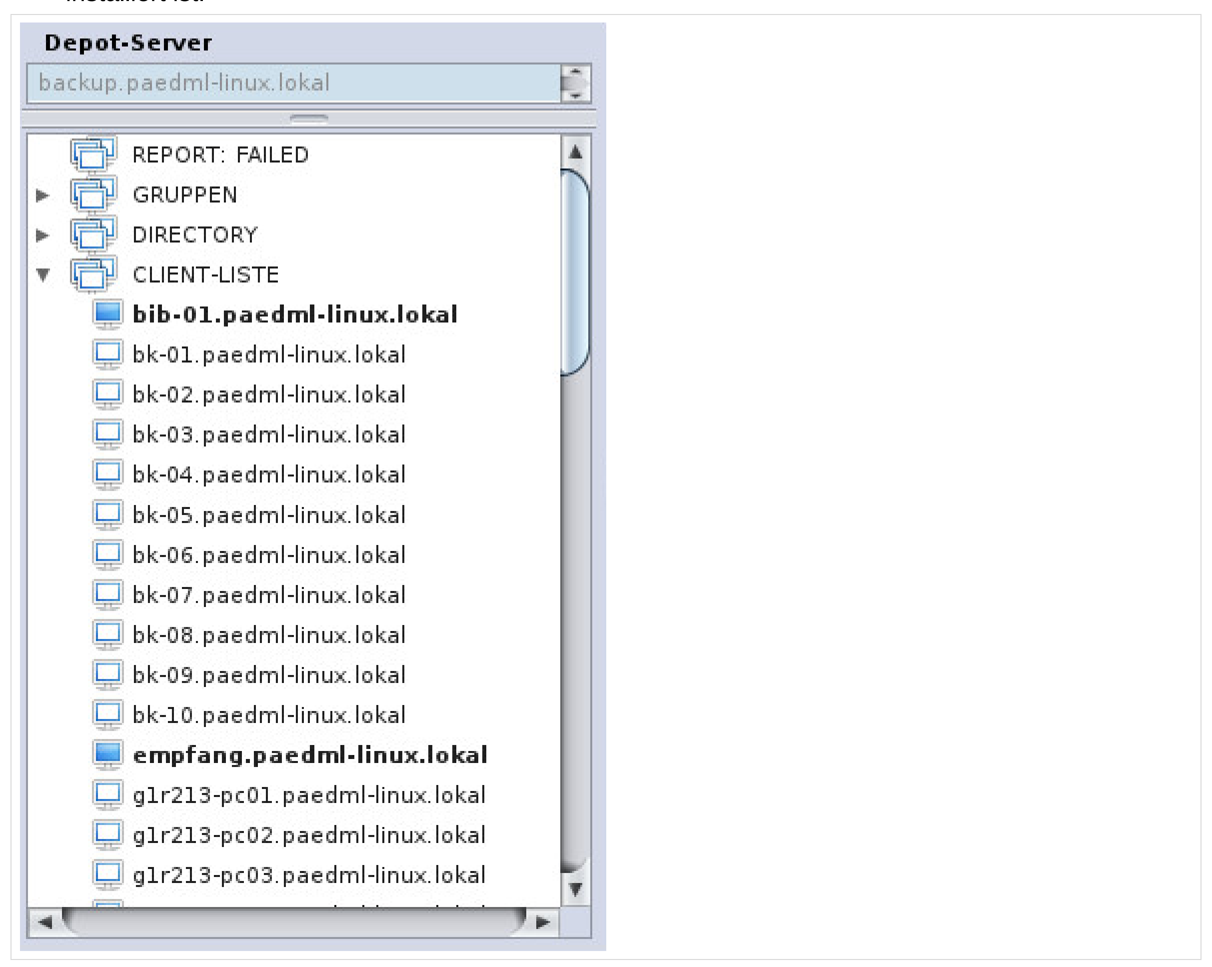


Abb. 128: opsi-config editor Detail – Auswahl einzelner Rechner

---

5. Das Hauptfenster ist in verschiedene Reiter unterteilt:



Abb. 129: Übersicht der Reiter im Hauptfenster

5.1. ✱ „*Clients*“: Hier finden Sie alle unter Punkt 4 ausgewählten Rechner.

5.2. ✱ „*Produktkonfiguration*“: Hier können Sie Software auf Rechner verteilen.

5.3. ✱ „*Netboot-Produkte*“: Dies sind Routinen, die über PXE-Boot verteilt werden können.

5.4. ✱ „*Host-Parameter*“: Hier finden Sie u.a. Parameter, die angepasst werden müssen, falls es Probleme beim Start von Rechnern gibt. Diese Funktion ist vergleichbar mit den Bootparametern unter *Linbo* in der *paedML Linux 5.x*. Nähere Informationen hierzu finden Sie in Kapitel 7.8.1 ab Seite 149.

5.5. ❋ „*Hardwareinformationen*“; Über das *Netboot-Produkt hwinvent* wird eine Liste der Hardwarekomponenten eines Clients erstellt. Diese Informationen werden zur Treiberintegration beim *Windows*-Rollout herangezogen.

5.6. ❋ „*Software-Inventur*“: Hier wird von *opsi* die am Client installierte Software aufgelistet. Hierfür muss auf den Clients das Programmpaket *swaudit* mindestens einmal installiert worden sein.

5.7. ★ „*Logdateien*“: Hier finden Sie verschiedene *opsi*-Logdateien. Der Log-Level kann angepasst werden.

5.8. ★ „*Produkt-Defaultproperties*“: Hier können Standard-Werte eingestellt werden, die den Produkten bei der Installation zugewiesen werden.

5.9. 💣 „*Depots*“: Hier kann zwischen verschiedenen *opsi*-Depots gewechselt werden. Der Knopf ist zunächst inaktiv, wird aber durch den Knopf „*Depoteigenschaften*“ (3.2) aktiviert. **Hier dürfen keine Werte verändert werden!**

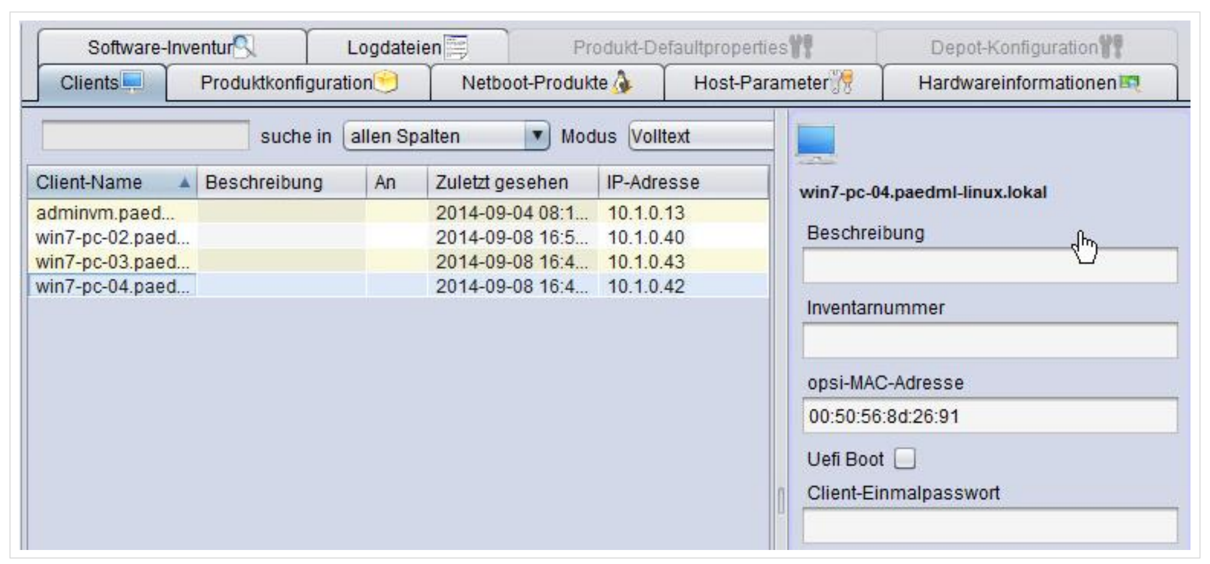


Abb. 130: opsi config editor Detail

---

6. Auf der rechten Seite finden Sie einen Bereich der – je nach Auswahl des *opsi*-Menüs – dynamisch befüllt wird. Hier können Parameter für die einzelnen *opsi*-Module eingesehen und bei Bedarf geändert werden.

7.4 Vervollständigen der opsi-Pakete für die Windows-Installation



Die Installationsroutine von *Microsoft Windows* benötigt Dateien, die aus lizenzrechtlichen Gründen nicht ausgeliefert werden dürfen. Im Folgenden wird beschrieben, was der Dienstleister tun sollte, damit die notwendigen Dateien auf dem *Backup*-Server ausgespielt werden.



Die *paedML Linux* unterstützt offiziell nur die deutschen Versionen von *Windows 7 Professional* (64-Bit) sowie *Windows 8.1 Pro* (64-Bit).

Windows XP funktioniert zwar mit der *paedML Linux*, aufgrund der von *Microsoft* eingestellten Entwicklung raten wir jedoch vom Einsatz von *XP* ab.

Statt *Windows XP* können Sie versuchen, *Windows 7* in der 32-Bit-Version einzusetzen. Dieses Betriebssystem kann in der Regel auf Rechnern, die über 1GB RAM verfügen, installiert werden[37].

Es gibt zwei Wege, wie Sie Installationsdateien in das *opsi*-Depot übertragen können. Sie können über *opsi-configed* Dateien auf den Server kopieren (folgender Abschnitt) oder die Daten über den *VMware vSphere Client* (vgl. Kapitel 7.4.2, ab Seite 133) in das System integrieren.

7.4.1 Bereitstellen von Installationsdateien über die opsi-Konsole



Nutzen Sie für die folgende Funktion die lokale Instanz des *opsi-configed*, da es bei der Web-Version zu Problemen bei der Datenübertragung kommen kann.

opsi-configed führt Sie mit dem Knopf „*Produktverwaltung*", in ein Dialogfenster, über das Sie *opsi-Pakete* installieren können. Sie können über diese Funktion *Localboot-Produkte* (vgl. Kapitel 7.13, Seite 157) auf den Server laden oder Installationsdateien für *Netboot-Produkte* vervollständigen. Sie finden den Knopf oben rechts in der *opsi*-Management-Konsole.

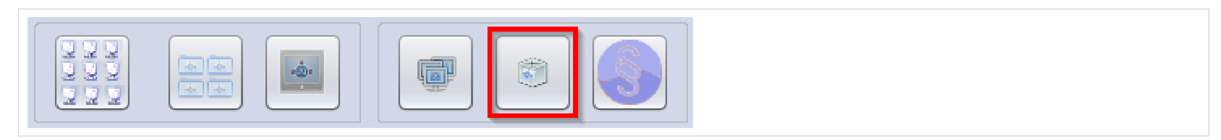


Abb. 131: Der Button „Produktverwaltung"

Im unteren Bereich des neuen Fensters („Vervollständigung eines *Windows*produkts") können Sie Ihre Anpassungen vornehmen. Auf dem Backup-Server finden sich im Ordner */var/lib/opsi/depot* Unterordner mit den *opsi*-Produkten. Neben den Programmpaketen (oder zum Beispiel 7-zip, Firefox,…) finden Sie dort Ordner, in denen die Netboot-Produkte („opsi-local-image-*") für die Betriebssysteminstallation liegen.



Damit Sie auf das *opsi-Depot* zugreifen können, müssen Sie an dem Arbeitsplatz, von dem Sie Änderungen vornehmen, als **Administrator der Domäne** angemeldet sein.

Für das Vervollständigen der Installationsdateien benötigen Sie einen Zugriff von der Maschine, mit der gearbeitet wird (zum Beispiel die „*AdminVM*" oder ein beliebiger Rechner anderer im Netz) auf die Installationsdateien. Diese können entweder als CD/DVD oder über ein Laufwerk zur Verfügung gestellt werden.

[37] Nähere Informationen hierzu unter http://*windows*.*microsoft*.com/de-de/*windows*7/products/system-requirements

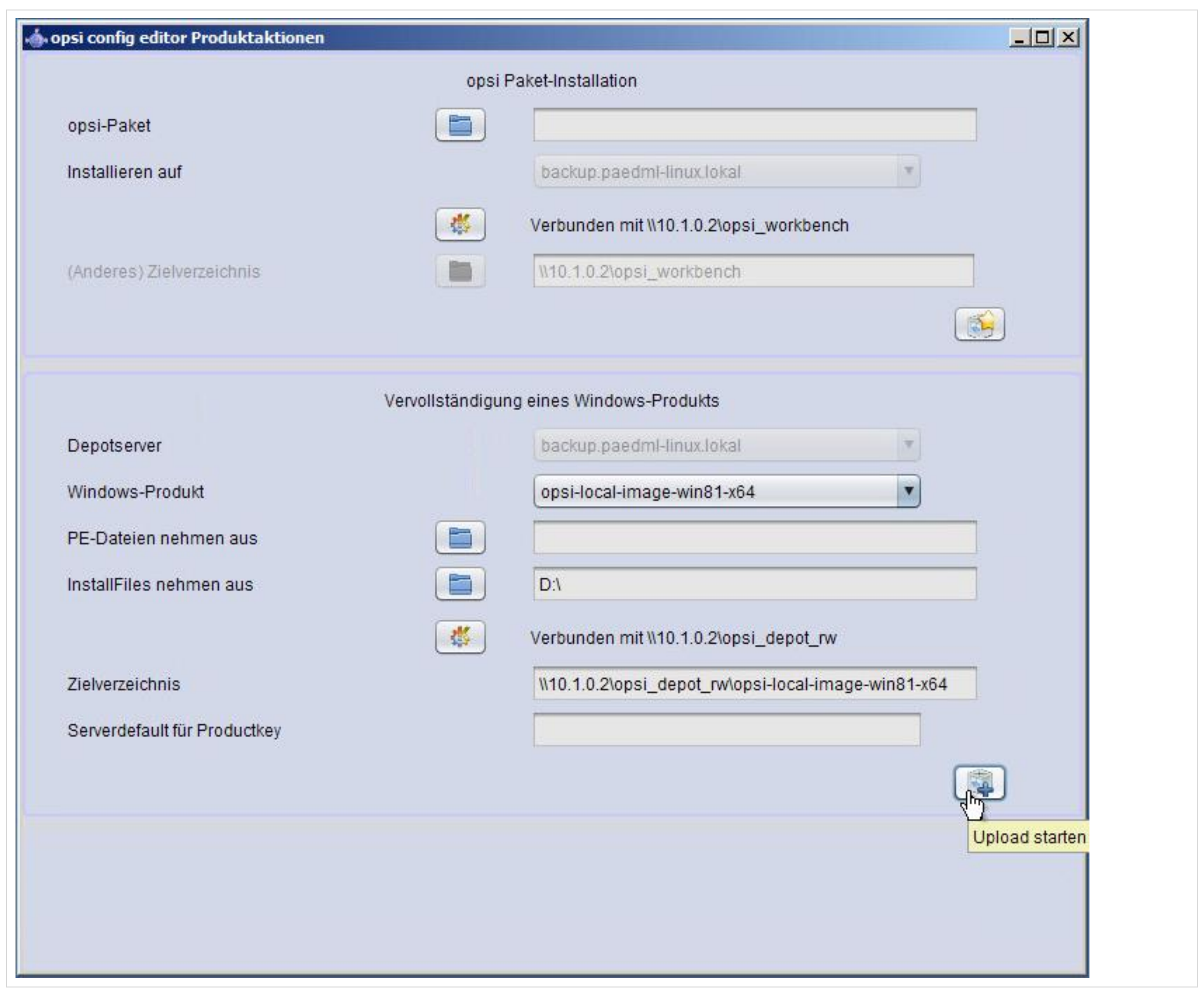


Abb. 132: Vervollständigung des Windows-*Produkts „opsi.local-image-win7-x64“*

Die folgenden Einträge sollten Sie vornehmen:

Feld	**Beschreibung**
Depotserver	Zielserver des *opsi*-Depots, nicht editierbar.
Windows-Produkt	Wählen Sie hier das *Netboot-Produkt* aus, das mit Daten versorgt werden soll.
PE-Dateien nehmen aus	*Windows*-PE-Dateien werden für die Installation von *Windows* benötigt. **Hier darf nichts geändert werden, da sich diese Dateien bereits auf dem Server befinden.**
InstallFiles nehmen aus	Geben Sie hier den Ort des Installationsmediums ein. (Im vorliegenden Beispiel Datenträger in *D:*\)
Ohne Beschriftung: Status des *opsi*-Depots	Hier sollte „*Verbunden mit \\10.1.0.2\opsi_depot_rw*“ stehen, damit die Daten übertragen werden können. Über den bunten Knopf kann ggf. eine Verbindung hergestellt werden. Sollte keine Verbindung zu stande kommen, hat der Benutzer, mit dem Sie am Rechner angemeldet sind, möglicherweise keinen Zugriff

	auf \\backup\opsi-depot-rw .
Zielverzeichnis (in *opsi_depot*)	Zielort des *opsi*-Depots, wird über die Auswahl des *Windows*-Produktes gefüllt.
Serverdefault für Productkey	Hier kann ein Lizenzschlüssel eingetragen werden. Dies ist aber in der Regel nicht notwendig, da die Aktivierung über VAMT (vgl. Kapitel 13 ab Seite 194) geschieht.

Tabelle 18 - Werte von Windows-*Produkten*

Wenn alle Werte entsprechend eingetragen wurden, können Sie das ausgewählte *Netboot-Produkt* auf dem Server vervollständigen. Drücken Sie hierfür auf den Knopf „*Upload starten*" unten rechts.

7.4.2 Bereitstellen der Installationsdateien über vSphere Client

Zur Installation von *Windows 7 Professional* bzw. *Windows 8.1 Pro* benötigt *opsi* alle Daten der Installations-DVD. Auf der DVD sollte das jeweils aktuelle Service Pack bereits enthalten sein.

Legen Sie die DVD in dem Computer ein, auf dem Sie den *VMware vSphere Client* ausführen und öffnen Sie die Konsole der *opsi-Server-VM*. Binden Sie nun das DVD-Laufwerk des Computers in die virtuelle Maschine ein, indem Sie auf das CD-Icon klicken und das passende Laufwerk verbinden.

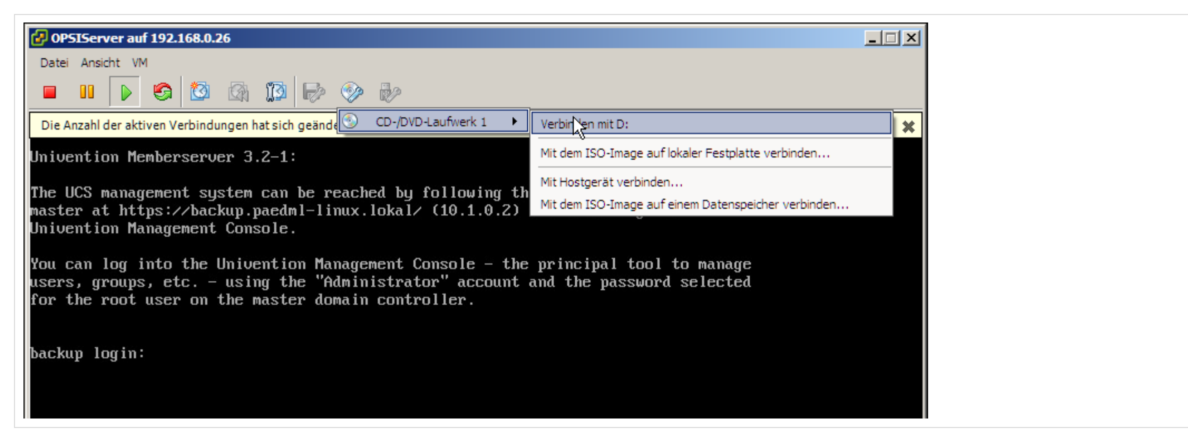


Abb. 133: DVD-Laufwerk verbinden

Melden Sie sich nun als Benutzer „`root`" an der *OPSI-Server-VM* an und führen Sie folgende Befehle aus:

1. Einhängen der CD:

```
#mount /cdrom
```

2. Kopieren der Daten für *Windows 7*:

```
#cp -r /cdrom/* /var/lib/opsi/depot/opsi-local-image-win7-x64/installfiles
```

oder für *Windows 8.1*:

```
#cp -r /cdrom/* /var/lib/opsi/depot/opsi-local-image-win81-x64/installfiles
```

3. Aushängen der CD:

```
#umount /cdrom
```

4. Setzen der Rechte der eben kopierten Daten für *Windows 7*:

```
#opsi-set-rights /var/lib/opsi/depot/opsi-local-image-win7-x64/installfiles
```

oder für *Windows 8.1*:

```
#opsi-set-rights /var/lib/opsi/depot/opsi-local-image-win81-
x64/installfiles
```

Trennen Sie abschließend das DVD-Laufwerk des Computers von der *OPSI-Server-VM*, indem Sie auf das CD-Icon klicken und das Laufwerk trennen.

7.5 Installation der Arbeitsplatzrechner

Nachdem im vorigen Abschnitt die Installationsdateien für die *Windows*installation bereitgestellt wurden, kann nun mit der Vorbereitung und dem Ausspielen der Arbeitsplatzrechner begonnen werden.

Bevor Clients jedoch mit *opsi* verwaltet werden können, müssen Sie am Server registriert werden (vgl. Kapitel 4.2 Seite 67 ff.). Bitte beachten Sie, dass Clients bei der Registrierung unbedingt mit dem *Systemtyp „Windows-System“* versehen werden müssen, damit Sie mit *opsi* verwaltet werden können.

Bei der Rechneraufnahme in die *paedML* wird ein Rechner-Objekt in der *opsi*-Datenbank erstellt. Diese Rechner erscheinen in der Rechner-Liste (3) und können dort ausgewählt werden.

In der *opsi*-Konsole können Sie definieren, mit welcher Software ein Rechner versorgt werden soll. Hierüber können Sie beispielsweise das Betriebssystem ausspielen (inklusive Anpassung der Partitionsgrößen), Softwarepakete installieren oder ein Programm anstoßen, das die Rechnerhardware inventarisiert (wichtig für die Integration von Treibern).

Die Installation der ausgewählten Pakete können Sie zu verschiedenen Zeitpunkten[38] starten:

1. sofort, sofern der Rechner gestartet ist,
2. sofort, sofern der Rechner ausgeschaltet ist und über PXE gebootet werden kann oder
3. beim nächsten Systemstart,



Die Einrichtung und Aufnahme von Rechnern in die *paedML* ist originäre Aufgabe des Dienstleisters.

[38] Die Installation bei laufenden Systemen oder über PXE-Boot kann „on demand“ über die opsi-Konsole angestoßen werden, ansonsten wird Software beim nächsten Systemstart installiert.

7.5.1 Automatische Installation

Es gibt die Möglichkeit, dass Sie die *paedML Linux* so konfigurieren, dass die Rechner nach der Rechner-Aufnahme und folgendem Neustart automatisch mit einem Betriebssystem[39] versorgt werden.

Dies vereinfacht die Erstinstallation eines Schulnetzes.



Um die automatische Installation zu aktivieren müssen Sie die *UCR*-Variable *lmz/import/rollout_client/* auf „*yes*" setzen (vgl. Kapitel 1.3.3, Seite 29). Dies muss geschehen, **BEVOR** die Rechner, die Sie automatisch ausrollen wollen, in die *paedML Linux* aufgenommen wird.

Wenn Sie die automatische Installation wieder deaktivieren wollen, setzen Sie den Wert der *UCR*-Variable *lmz/import/rollout_client/* auf „*no*".

Wenn die automatische Installation aktiviert ist, wird – nach der Aufnahme eines *Windows*-Rechners – dieser automatisch für die Installation von *Windows 7* (64-Bit) mit den folgenden Parametern markiert:

- Partitionierung (40 Gigabyte Systempartition, Null Gigabyte Datenpartition)
- *Windows 7* (ohne extra Treiber)
- Folgende *opsi*-Softwarepakete werden installiert:
  - „*clientprodukte*" (Sammlung der für den Betrieb der paedML nützlichen Programmen und *Windows*-Hotfixes)
  - „*windomain*" – Paket für den Domänenbeitritt



ACHTUNG. Bei der Partitionierung werden alle Daten auf der Festplatte überschrieben!

Wenn Sie ein anderes Betriebssystem als *Windows 7* installieren wollen, müssen Sie sich als Benutzer „*root*" an der Konsole des Backup-Servers anmelden und den folgenden Befehl ausführen (der Befehl muss am Stück eingegeben werden, der Umbruch ist darstellungsbedingt):

```
#opsi-admin -d method productPropertyState_create opsi-local-image-prepare
start_os_installation backup.paedml-linux.lokal 'PRODUKTNAME'
```

Ersetzen Sie *PRODUKTNAME* durch das gewünschte *Windows*-Netbootprodukt. Zur Auswahl stehen derzeit

- *Windows 7* (32 Bit) (opsi-local-image-win7)
- *Windows 7* (64 Bit) (opsi-local-image-win7-x64)
- *Windows 8.1* (opsi-local-image-win81-x64)

---

[39] Alle Installationsdateien für *Windows* müssen, wie im vorhergehenden Unterkapitel beschrieben, erst noch auf dem OPSI-Server hinterlegt werden.

Wenn Sie also *Windows 8.1* installieren wollen, setzen Sie den folgenden Befehl an der Konsole ab:

```
#opsi-admin -d method productPropertyState_create opsi-local-image-prepare
start_os_installation backup.paedml-linux.lokal 'opsi-local-image-win81-
x64'
```

Das Ändern der Partitionsgröße führen Sie mit dem folgenden Befehl aus (ersetzen Sie „WERT_IN_GB“ durch die gewünschte Größe der Partition – zum Beispiel „*70G*“ für eine Partition mit 70 Gigabyte):

```
#opsi-admin -d method productPropertyState_create opsi-local-image-prepare
system_partition_size backup.paedml-linux.lokal 'WERT_IN_GB'
```

Um eine Datenpartition anzulegen, führen Sie den folgenden Befehl aus (ersetzen Sie „WERT_IN_GB“ durch die gewünschte Größe der Partition – zum Beispiel 70G für eine Partition mit 70 Gigabyte):

```
#opsi-admin -d method productPropertyState_create opsi-local-image-prepare
data_partition_size backup.paedml-linux.lokal 'WERT_IN_GB'
```

7.5.2 Manuelle Installation



Beachten Sie, dass bei einem mit opsi verwalteten Rechner (Windows-)Updates nicht manuell oder automatisch eingespielt werden dürfen.

Spielen Sie (*Windows*-)Aktualisierungen **NUR** über *opsi* ein. „*hotfix*“-Pakete (*Windows*-Updates) oder aktualisierte Pakete im *opsi-Depot* beinhalten diese Updates.

Um Computer Ihres schulischen Netzes zu installieren, markieren Sie diese in der Rechnerliste (4).

Im Hauptfenster (5) wählen Sie den Reiter „*Netboot-Produkte*“.

Wir empfehlen, die Installation der Rechner immer mit dem „*Netboot-Produkt*“ „*opsi-local-Image-prepare*“ durchzuführen. Mit diesem *opsi*-Werkzeug wird eine Festplatte dergestalt eingerichtet, dass die Festplatte in verschiedene Bereiche partitioniert wird.

opsi-local-image-prepare arbeitet mit einem statischen Partitionskonzept (vgl. die folgende Grafik):

- Auf der *System-Partition* liegt das Betriebssystem mit allen Programmdateien.
- Bei jeder Partitionierung wird eine *Hilfs-Partition* angelegt, die für die Ablage der Installationsdateien des Betriebssystems genutzt wird. Linux-Systeme könnten diese Partition später als *Swap-Partition* verwenden.
- Die optionale *Daten-Partition* kann eingerichtet werden, um Festplattenplatz für Projekte bereit zu stellen. So kann man zum Beispiel Videoprojekte dauerhaft Daten auf der *Daten-Partition* ablegen und lokal damit arbeiten. Der Austausch großer Datenmengen mit dem Server kann so verhindert werden.

- Ein zentraler Bestandteil der Installation mit „*opsi-local-image-prepare*“ ist das Erstellen einer *Backup-Partition*. In dieser *Backup-Partition* werden lokale Images der Rechner vorgehalten (vgl. Kapitel 9 ab Seite 167).



Achtung! Die optionale Datenpartition muss gesondert gesichert werden – natürlich nur, wenn Sie die Daten gesichert haben wollen.

Ein Problem bei Datenpartitionen ist, dass sie im Klassenarbeitsmodus NICHT deaktiviert werden. Dadurch können Schüler „virtuelle Spickzettel“ erstellen und damit arbeiten.

Außerdem wird die Datenpartition nicht von der paedML verwaltet. Alle dort abgelegten Daten bleiben unangetastet, bis sie händisch gelöscht werden oder das System mit Hilfe des *Netboot-Produktes opsi-local-image-prepare* neu installiert wird.

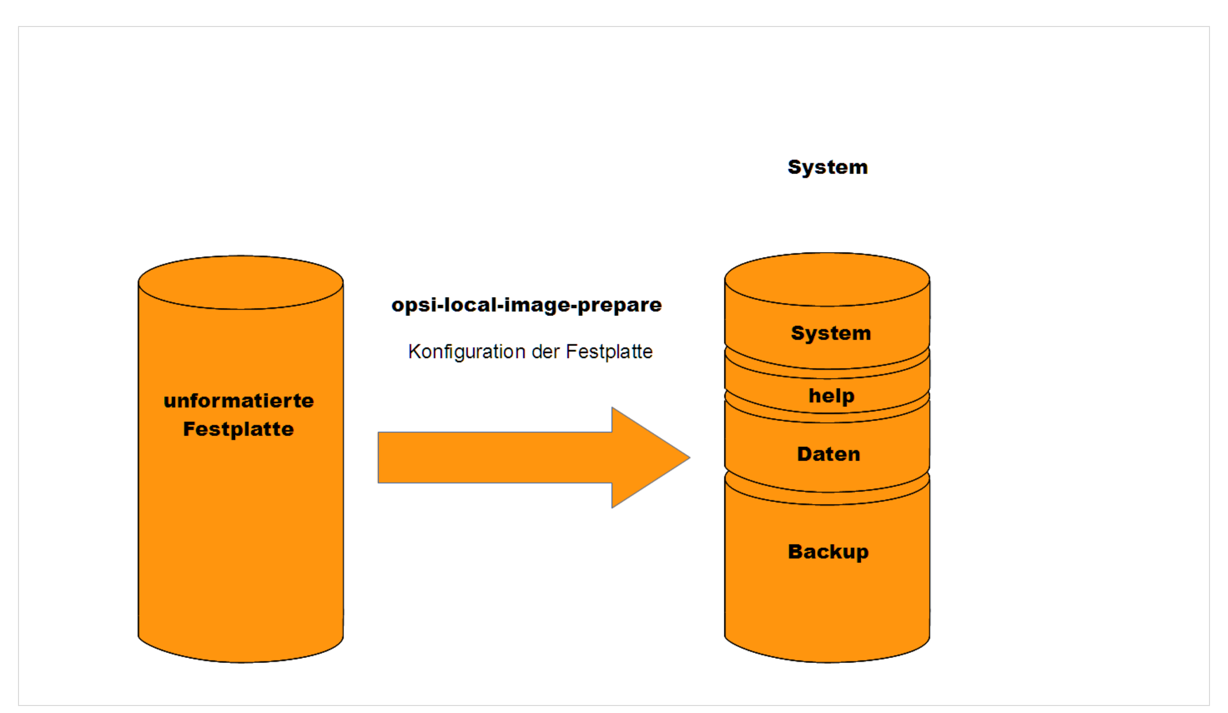


Abb. 134: Konfiguration der Festplatte mit opsi-local-image-prepare

Bei der Einrichtung eines Rechners können Sie verschiedene Anpassungen an *opsi-local-image-prepare* vornehmen. Wählen Sie das Produkt aus uns klicken Sie in die Spalte „*Angefordert“*. Wählen Sie dort den Eintrag „*Setup“*.

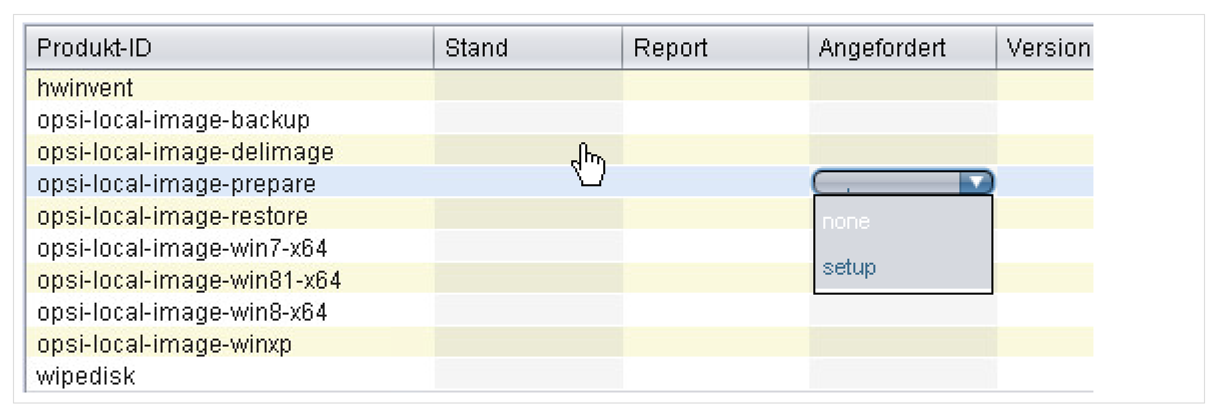


Abb. 135: Auswahl von opsi-local-image-prepare für die Windows*installation*

Der dynamische Inhalt der *opsi*-Konsole (6) wird mit Informationen zum *Netbootprodukt* und mit Parametern (Bereich: „*Konfiguration für Client*“) gefüllt, die angepasst werden müssen. Die Einstellungen können wie folgt vorgenommen werden:

Property-Name	**Property-Wert**
askbeforeinst	Hier kann eine Bestätigung vor der Installation am Arbeitsplatzrechner eingebaut werden. Sofern der Wert auf „*false*“ belassen wird (empfohlen), läuft die Installation automatisch durch. Bei der Installation wird die Festplatte komplett formatiert!
data_partition_size	(optional) – Wie groß soll eine Datenpartition angelegt werden. Der *Property-Wert* für *data_partition_size* ist im Standard auf *0G* gestellt. Wobei *G* für Gigabyte steht. Wenn Sie Datenpartitionen anlegen wollen, müssen Sie diesen Wert entsprechend ändern.
start_os_installation	Hier wird ausgewählt, welches Betriebssystem installiert werden soll.
system_partition_size	Wie groß soll die Systempartition angelegt werden? Der *Property-Wert* für *system_partition_size* ist im Standard auf *40G* gesetzt. Wählen Sie hier einen anderen vordefinierten Wert oder geben Sie eine eigene Partitionsgröße ein, falls Sie Ihre *Windows*-Partition größer anlegen wollen.

Tabelle 19: Parameter von „opsi-local-image-prepare“

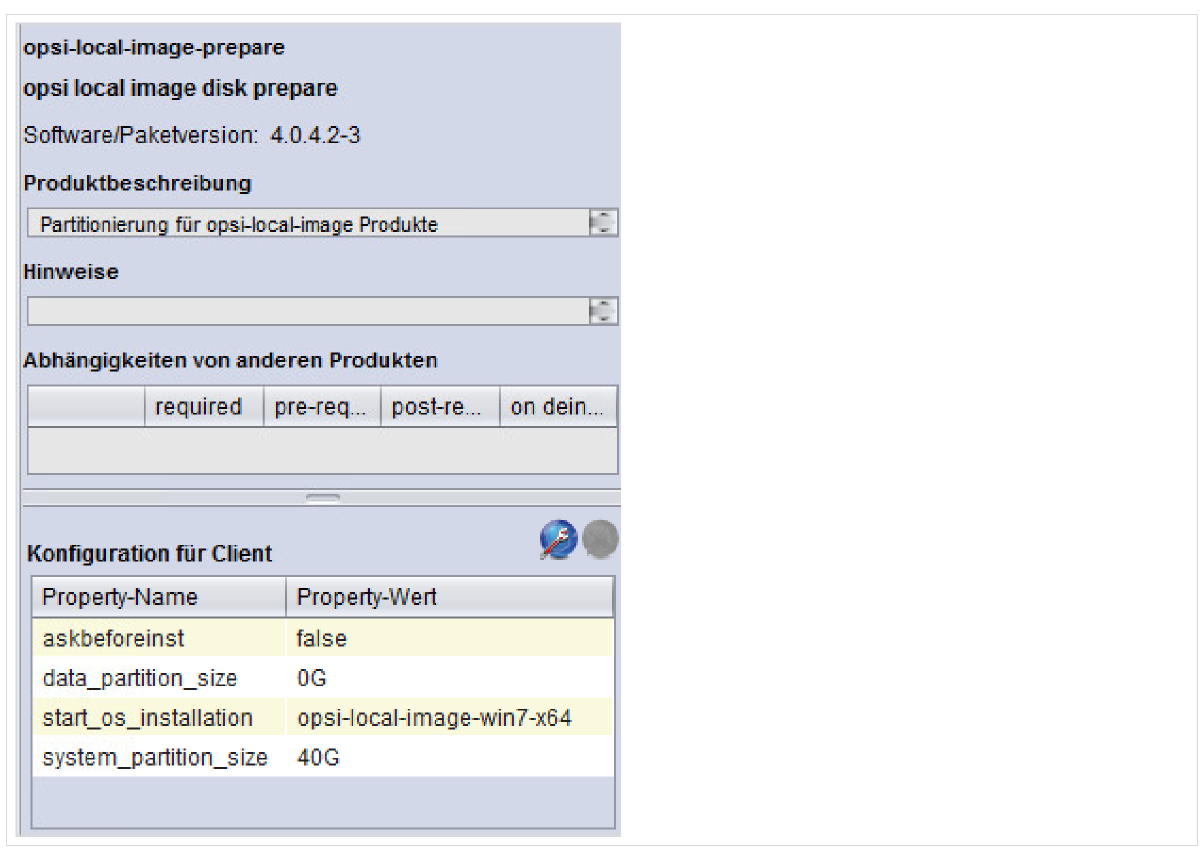


Abb. 136: Einstellungen für „opsi-local-image-prepare“

Das Feld „*start_os_installation*“ wird mit den auf dem Backup-Server installierten *Windows*abbildern befüllt. Dieser Wert ist daher abhängig von der Einrichtung der Installationsdateien, die Sie in Kapitel 7.4 vorgenommen haben. Zu jeder installierten *Windows*version gibt es ein eigenes *Netboot-Produkt „opsi-local-image-VERSION*“, das Sie für die Installation auswählen können.

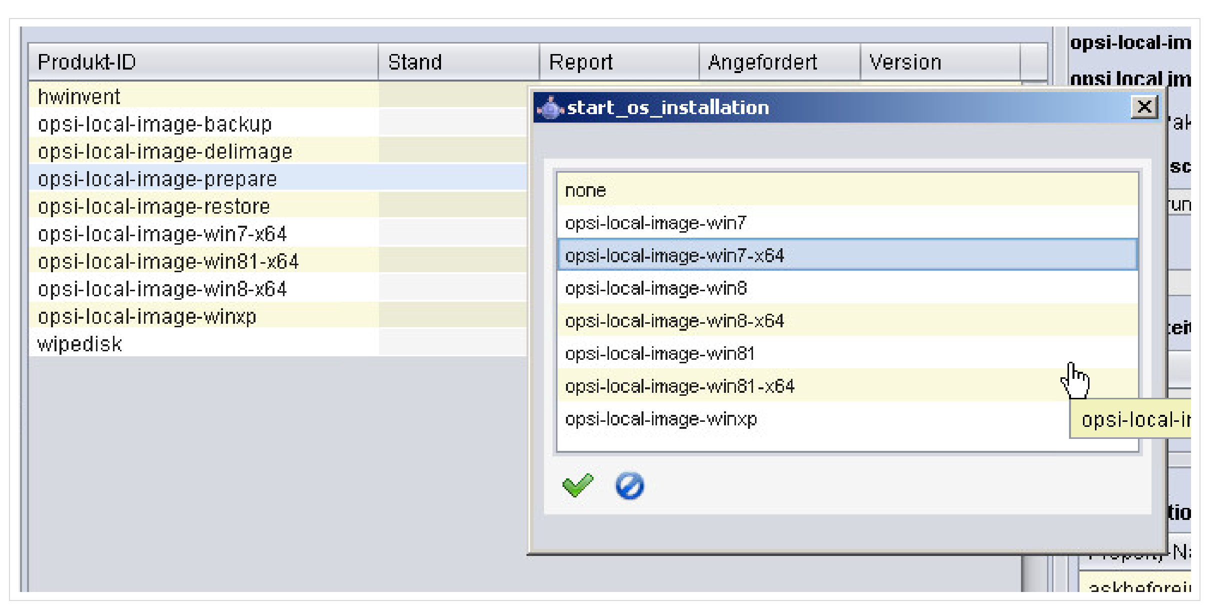


Abb. 137: Auswahl des zu installierenden Betriebssystems

Alle Änderungen müssen anschließend mit dem *roten Haken* unter (2) gespeichert werden.



Abb. 138: Der rote Haken zeigt an, dass Änderungen noch nicht übernommen wurden.

Wenn die Werte übernommen wurden, wird der Haken *grün*.



Abb. 139: Änderungen wurden übernommen.

Vor der Installation der Rechner können Sie im Reiter „*Produktkonfiguration*“ auswählen, welche Software Sie installieren wollen (vgl. Kapitel 7.9).

Beim nächsten Clientstart wird die Installation angestoßen, sofern der Client über PXE bootet. Das System wird ggf. automatisch neu gestartet, um die Installation durchzuführen.

Die Zuweisung spezieller Treiber geschieht über das Netboot-Produkt, welches im Feld „*start_os_installation*“ angegeben wird. Das Ausspielen spezieller Geräte-Treiber ist Gegenstand des folgenden Abschnittes.

7.6 opsi-Standard-Einstellungen („Produkt-Defaultproperties“)

Die meisten *opsi*-Produkte können bei der Installation angepasst werden. So gibt es für bestimmte Programme die Option bei der Installation einen Proxy einzurichten. Für das *Netboot-Produkt „opsi-local-image-prepare*“ kann eingestellt werden, wie groß Festplattenpartitionen angelegt werden sollen.

Bevor ein *opsi*-Produkt ausgespielt wird, können Sie die „*Property-Konfiguration*“, also die konfigurierbaren Werte für die zur Installation vorgesehenen Programme ändern.



Die *Property*-Konfiguration gilt zunächst global. Dies bedeutet, dass alle Rechner mit den vordefinierten Werten installiert werden.

Produkt-Properties können aber auch für ausgewählte Clients gesetzt werden. Diese Werte können bei der Installation des jeweiligen Produktes angepasst werden. In diesem Fall wirken sich nachträgliche Änderungen an den Default-Properties NICHT auf diese Rechner aus.

Um die Standard-Einstellungen dauerhaft zu ändern, müssen diese im Reiter „*Produkt-Default-Properties*“ eingestellt werden. Der Reiter „*Produkt-Defaultproperties*“ im Hauptfenster (5) ist zunächst inaktiv und wird erst durch das Anklicken der Schaltfläche „*Depoteigenschaften*“ verfügbar.



Abb. 140: Zugriff auf „Produkt-Defaultproperties“ über die „Depoteigenschaften“



Im Reiter „*Depot-Konfiguration*“, der ebenfalls nach dem Klick auf „*Depoteigenschaften*“ verfügbar ist, **darf NICHTS geändert werden.**

Um die Parameter eines *opsi*-Produktes dauerhaft zu verändern, wählen Sie das Produkt aus. Alle konfigurierbaren Werte (die sogenannten „*Produkt-Properties*“) finden Sie nach Auswahl des *opsi*-Produktes im dynamischen Bereich (6) der *opsi*-Konsole.

Im folgenden Beispiel wird die Größe der Systempartition von *Windows*-Installationen angepasst. Geänderte Werte werden fett hervorgehoben.

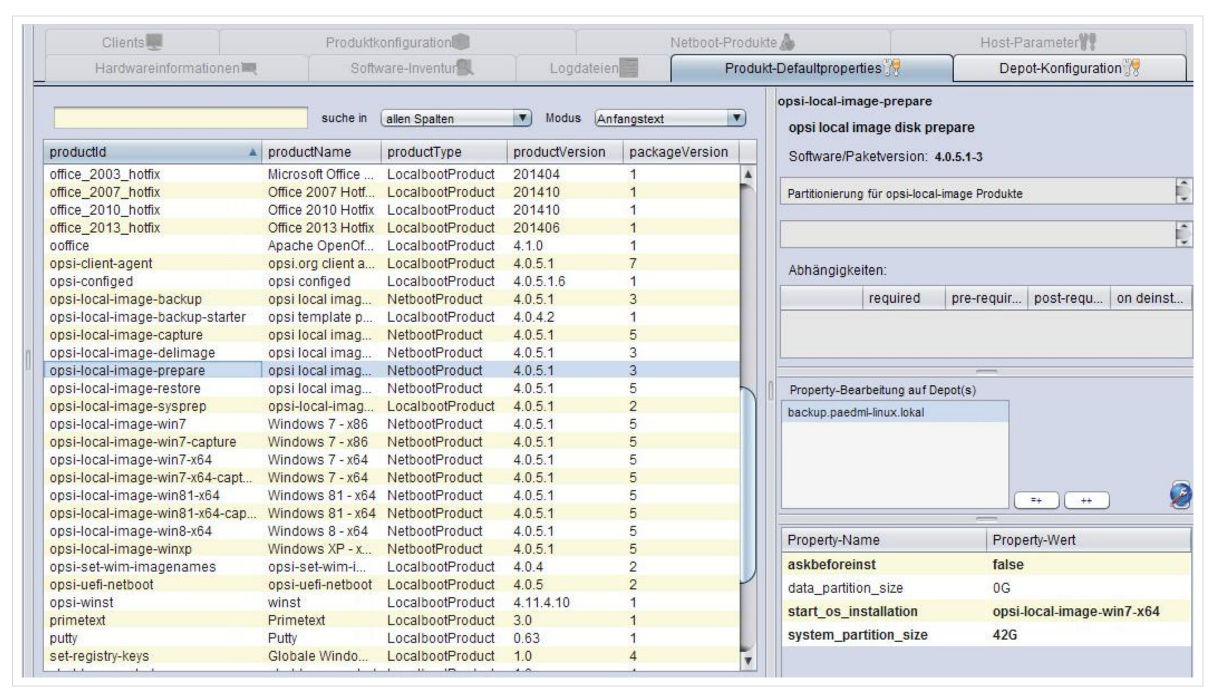


Abb. 141: Auswahl des opsi-Produktes

Die Produkteigenschaften können Sie ändern, indem Sie den zu ändernden Wert mit einem Doppelklick in der Spalte „*Property-Wert*“ öffnen. Sie können einen der vordefinierten Werte übernehmen oder einen neuen Index-Eintrag erstellen. Letzteres geschieht, in dem Sie den neuen Wert in das leere Feld eintragen (im folgenden Screenshot soll die Systempartition auf 42G(igabyte) erhöht werden) und auf das *gelbe Plus-Zeichen* drücken. Der neue Wert wird in die Liste der auswählbaren Werte übernommen und kann ausgewählt werden.

Ein Klick auf den grünen Haken übernimmt den selektierten Eintrag als „*Default-Produkproperty*“. Künftig werden alle Installationen von opsi-Produkten – bis zu nächsten Änderung – mit dem neu definierten Wert ausgeführt.

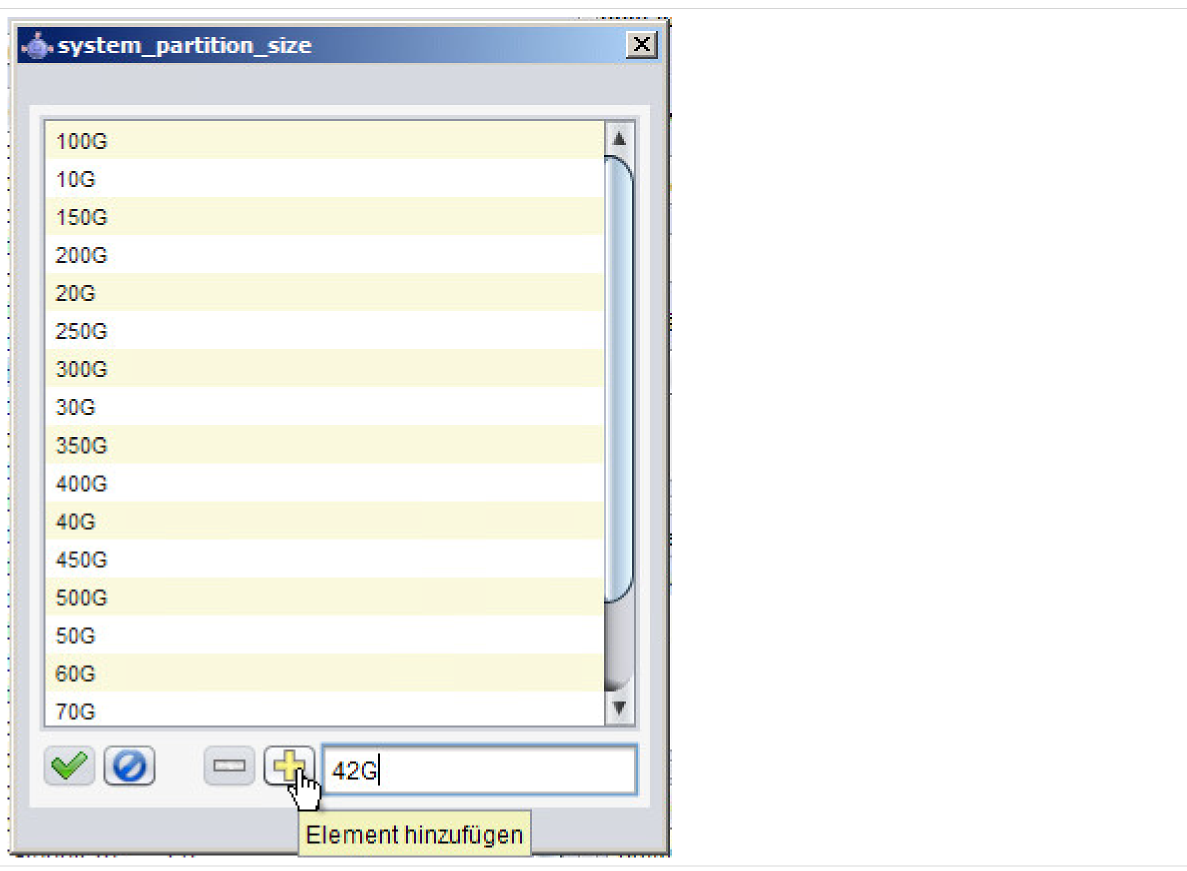


Abb. 142: Eintragen eines neuen Wertes für die Partitionsgröße

Wenn die Depot-Eigenschaften konfiguriert werden, sind alle anderen *opsi*-Reiter ausgegraut. Sie können die Reiterauswahl wieder rückgängig machen, in dem Sie auf den Knopf „*Client-Konfiguration*“ klicken.

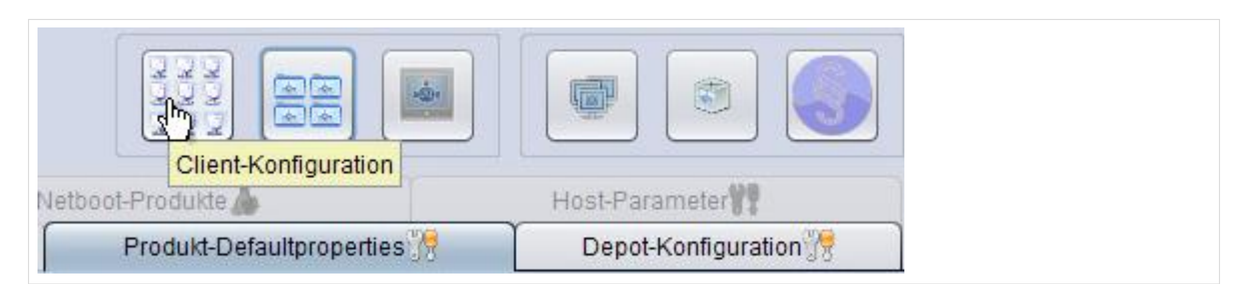


Abb. 143: Zugriff auf die opsi-Standardreiter via „Client-Konfiguration“

7.7 Treiberintegration

Ein häufig anzutreffendes Problem bei der Installation von Betriebssystemen sind fehlende Treiber. Heterogene Clients mit unterschiedlichen Hardware-Komponenten, exotische Chipsätze,

unterschiedliche Betriebssysteme,… Die Faktoren, die einen Administrator zur Verzweiflung bringen können, sind vielfältig.

Leider kann dieses Problem auch durch den Einsatz von *opsi* nicht gelöst werden, so dass die Suche nach fehlenden Treibern immer noch Aufgabe des Administrators bleiben wird! Was *opsi* aber bietet ist das zentrale Bereitstellen von Treibern[40], die bei der Installation automatisiert auf den Clients installiert werden.

Wenn kein Treiber für eine Komponente auf dem *opsi*-Server gefunden wurde, dann bricht die Installation entweder ab oder es wird ein Eintrag in den *opsi*-Logdateien erstellt, in dem auf den nicht vorhandenen Treiber hingewiesen wird.

```
(…)
[6] [Feb 24 11:14:22] Searching driver for PCI_DEVICE '3rd Gen Core
processor Graphics Controller', id '8086:0166' (WindowsDrivers.py|94)

[3] [Feb 24 11:14:22] PCI_DEVICE vendor directory 'opsi-local-image-win81-
x64/drivers/pciids/8086' not found (WindowsDrivers.py|108)
(…)
```



Die Log-Dateien des Systems sollten auf Einträge, wie die im folgenden Screenshot gezeigten, untersucht werden. Damit kann sichergestellt werden, dass die Installation aller Treiber auf den Rechnern durchgelaufen ist.

Sie finden die entsprechenden Einträge im *opsi-Hauptfenster* (5) im Reiter „*Logdateien*" und dort im Unterreiter „*boot-Image*".

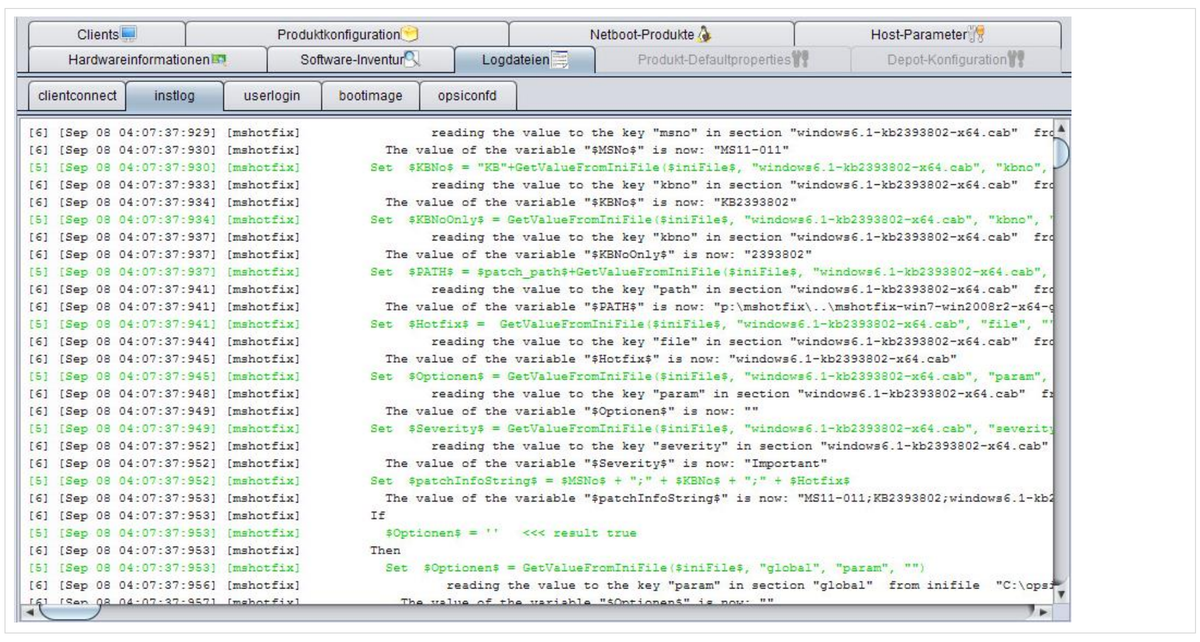


Abb. 144: Ansichtsfenster der Logdateien

[40] In Netboot-Produkten zu XP und *Windows* 7 sind einige gängige Hardwaretreiber enthalten.

Wenn bei der Installation nicht automatisch die Treiber aller Komponenten eines Rechners gefunden werden, dann haben Sie verschiedene Möglichkeiten, eigene Treiber auf einem Arbeitsplatzrechner zu integrieren:

1. *Treiber händisch nachinstallieren* – nicht wirklich eine Lösung, da in der Regel zu aufwändig, vor allem, wenn mehrere Rechner installiert werden müssen! Das unten beschriebene Verfahren der lokalen Imageerstellung (vgl. Kapitel 9 ab Seite 167) kann das Arbeitsergebnis dann aber sichern.
2. *Nachträgliche Installation eines Treibers als opsi-Programmpaket*. Wenn ein Treiber als .exe-Datei oder msi-Paket vorliegt, dann kann der Treiber zu einem *opsi*-Paket umgewandelt und über die *opsi*-Konsole verteilt werden. **Das Erstellen und die Einbindung eigener Pakete wird nicht durch die Hotline unterstützt.**
3. *Einspielen von Treibern auf den opsi-Server und (Neu-)Installation des Rechners mit allen Treibern*.

Wir empfehlen die dritte Option, die im Folgenden beschrieben wird.

7.7.1 Identifizieren von Treibern

Am einfachsten ist es natürlich, Treiber vom Hersteller direkt per Datenträger einzubinden. Bei Neugeräten sollten in der Regel Treiber vom Hersteller mitgeliefert werden, die Sie auf den Backup-Server übertragen können.

Wenn Sie das Problem haben, dass die Arbeitsplatzrechner nicht automatisch mit allen Treibern versorgt werden und Sie keine Hersteller-CD zur Hand haben, stellt sich die Frage, um welche Treiber es sich handelt, die nicht installiert werden können. opsi bietet hier die komfortable Möglichkeit, dies herauszufinden.

Das *opsi-Netbootprodukt hwinvent* liest die Hardwareinformationen der Arbeitsplatzrechner aus und stellt diese im Reiter „Hardwareinformationen“ im Hauptfenster (5) dar. Das Programm läuft automatisch bei jeder Installation, kann aber auch händisch gestartet werden. Wählen Sie das Produkt im Reiter „*Netboot-Produkte*“ aus und stellen Sie den Wert in der Spalte „*Angefordert*“ auf „*setup*“.

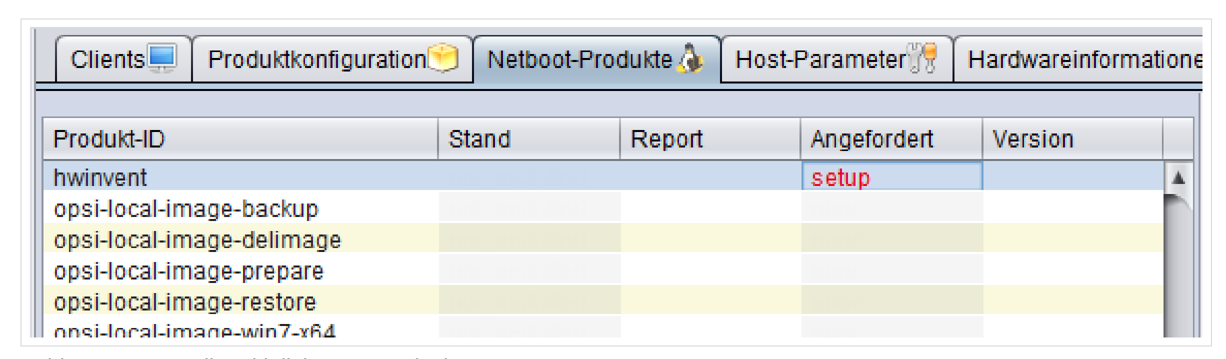


Abb. 145: Manuelle Initialisierung von hwinvent

Wenn *hwinvent* erfolgreich ausgeführt wurde, wird der Reiter „*Hardwareinformationen*“ befüllt. Anschließend können Sie beispielsweise das Computermodell in Erfahrung bringen und beim Hersteller nach Treibern suchen.

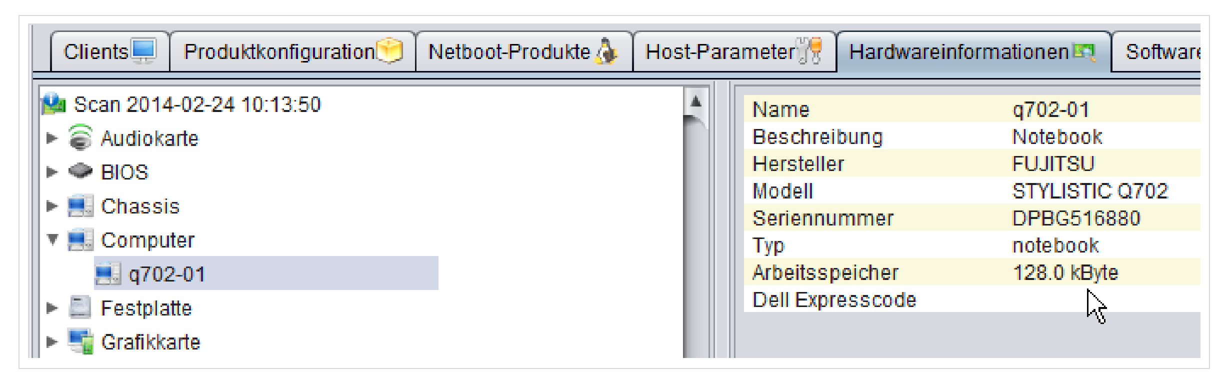


Abb. 146: Anzeige des Computermodells

Sie können sich aber auch gezielt Komponenten anzeigen lassen und nach Treibern suchen. Dies ist zum Beispiel sinnvoll, wenn Rechner nicht als Gesamtpaket gekauft, sondern zusammengestellt wurden.

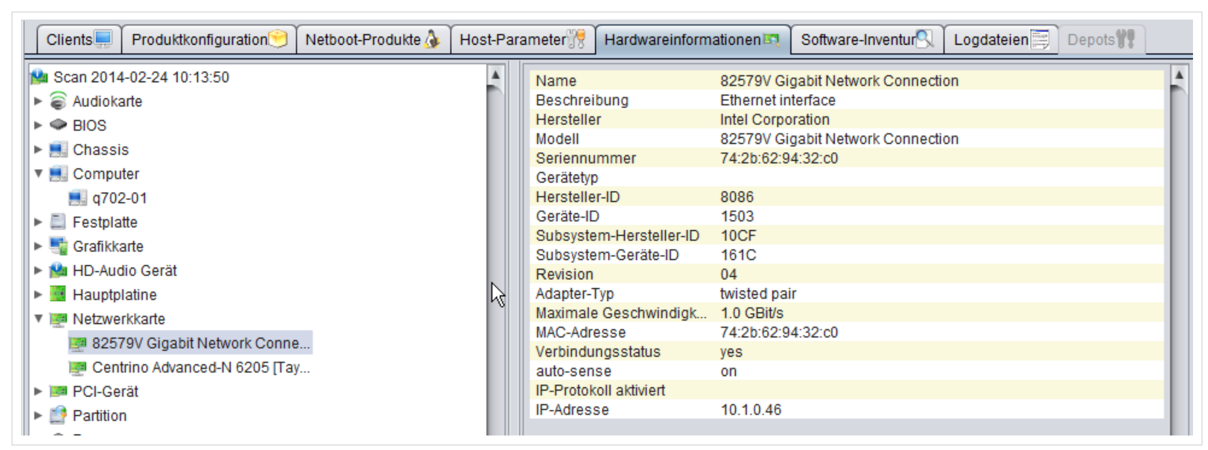


Abb. 147: Anzeige einzelner Hardwarekomponenten

7.7.2 Ausspielen von Treibern in das opsi-Depot

Alle manuell einzuspielenden Treiber müssen auf den Server übertragen werden (vgl. Kapitel 1.4.3, S 33 ff.).

Im Verzeichnis */var/lib/opsi/depot/* liegen alle Daten für die Betriebssysteminstallation, die Sie wie in Kapitel 7.4, Seite 130 ff. beschrieben auf dem Server angelegt haben.

Für jedes dieser Betriebssysteme müssen die dem Betriebssystem entsprechenden Treiber zur Verfügung gestellt werden. Die Treiber werden in das Verzeichnis */var/lib/opsi/depot/OS-NAME/drivers/drivers/* kopiert, wobei *OS-NAME* durch den von Ihnen für das jeweilige Betriebssystem erstellten Ordnernamen ersetzt werden muss.



Achten Sie darauf KEINE Umlaute, KEINE Sonderzeichen sowie KEINE Leerzeichen beim Anlegen der Treiberverzeichnisse zu verwenden.

Ein Beispiel: Die Treiber für die *Windows* 8.1 Installation werden nach */var/lib/opsi/depot/opsi-local-image-win81-x64/drivers/drivers* kopiert.

Die Ablage der Treiber kann in verschiedenen Ebenen geschehen:

1. *Allgemeine Treiber Pakete* – Wenn die Hardwareausstattung sehr heterogen ist, kann es sinnvoll sein, mit allgemeinen Treiberpaketen zu arbeiten. Allgemeine Treiber legen Sie ab unter *./drivers/drivers*. Nachteil dieser Methode ist, dass sich hier auch Treiber finden, welche zwar von der Beschreibung zu Ihrer Hardware passen, aber nicht unbedingt mit Ihrer Hardware funktionieren.
2. *Treiber die zu Ihrer Hardware gehören, aber nicht speziell zugeordnet sind* – Haben Sie nur wenige unterschiedliche Hardware zu unterstützen, so können Sie die Treiber in jeweils eigene Verzeichnisse (Name und Tiefe der Verzeichnisstruktur egal) unterhalb des Verzeichnisses *./drivers/drivers/preferred* ablegen.

   Treiber, die im Verzeichnis *./drivers/drivers/preferred* liegen, werden gegenüber den Treibern in *./drivers/drivers/* bevorzugt. Sie werden anhand der PCI-Kennungen (bzw. USB- oder HD_Audio-Kennung) in der Beschreibungsdatei des Treibers als zur Hardware passend erkannt und in das *Windows*-Setup mit eingebunden.

   Finden sich z.B. zu ein und derselben PCI-ID unterschiedliche Treiber unter *preferred*, so kann dies zu Problemen bei der Treiber-Zuordnung führen. In diesem Fall ist eine direkte Zuordnung der Treiber zu den Geräten notwendig.
3. *Treiber, die manuell Rechnern zugeordnet sind* – Zusätzliche Treiber, die unabhängig von ihrer Zuordnung bzw. Erkennung über die PCI- oder USB-IDs installiert werden sollen, gehören in jeweils eigene Verzeichnisse (Name und Tiefe der Verzeichnisstruktur egal) unterhalb des Verzeichnisses *./drivers/drivers/additional*.

   Über das *Produkt-Property „additional_drivers*“ des jeweiligen *Netboot-Produktes* können Sie einen oder mehrere Pfade von Treiberverzeichnissen innerhalb von *./drivers/drivers/additional* einem Client zu ordnen. Im Produkt-Property „*additional_drivers*“ angegebene Verzeichnisse werden rekursiv durchsucht und alle enthaltenen Treiber eingebunden.

   Dabei werden auch symbolische Links verfolgt. Dies können Sie nutzen, um für bestimmte Rechner-Typen ein Verzeichnis zu erstellen (z.B. dell-optiplex-815). Wird in den über „*additional_drivers*“ angegebenen Treiberverzeichnissen ein Treiber für ein vorhandenes PCI-Gerät (oder HD-Audio, USB) gefunden, so wird für dieses Gerät kein weiterer Treiber aus *drivers/preferred/* oder *drivers/* mehr eingebunden.

   Damit hat „*additional_drivers*“ nicht nur die Funktion, Treiber hinzuzufügen, welche über die normale Treibererkennung nicht gefunden würden. Darüber hinaus haben die Treiber, welche dem Client via „*additional_drivers*“ zugeordnet werden, auch Vorrang vor Treibern aus anderen Verzeichnissen.
4. *Treiber, die über die Felder <Hersteller>/<model> der Inventarisierung (hwinvent) automatisch den Rechnern zugeordnet werden* – Der im vorigen Abschnitt beschriebene Mechanismus der direkten Zuordnung von Treibern zu Geräten, kann automatisiert werden.

   Dazu wird während der Installation im Verzeichnis *./drivers/drivers/additional/byAudit* nach einem Verzeichnisnamen gesucht, der dem bei der Hardwareinventarisierung gefundenen Hersteller entspricht. In diesem „Vendor“ Verzeichnis wird nun nach einem Verzeichnisnamen gesucht, der dem bei der Hardwareinventarisierung gefundenen Modell entspricht. Wird ein solches Verzeichnis gefunden, so wird dieses Verzeichnis genauso behandelt, als wären sie über das *Produkt-Property „additional_drivers*“ manuell zugewiesen.

   Einige Hersteller verwenden Modellbezeichnungen, die für diese Methode sehr ungünstig sind, da man einige Sonderzeichen wie / nicht in Datei- oder Verzeichnisnamen verwenden darf. Ein Beispiel dafür wäre als Modelbezeichnung: "5000/6000/7000". Ein Verzeichnis mit dieser Bezeichnung ist wegen der Sonderzeichen nicht gestattet.

   In *opsi* werden deshalb folgende Sonderzeichen: < > ? " : | \ / * intern durch ein _ ersetzt. Mit dieser Änderung kann man oben genanntes schlechtes Beispiel als: "5000_6000_7000" anlegen und das

Verzeichnis wird automatisch zugewiesen, obwohl die Informationen in der Hardwareinventarisierung nicht der Verzeichnisstruktur entsprechen.

Im Folgenden wird das dritte Verfahren der obigen Liste, also das Installieren von Hardwaretreibern über die manuelle Zuordnung von Gerätetreibern zu Rechnern, beschrieben. In diesem Beispiel geschieht die Installation auf ein Fujitsu Tablet mit einem 64-Bit *Windows* 8.1.



Wir empfehlen, die Treiberintegration über die manuelle Zuweisung von Treibern an Rechner (drittes Verfahren aus vorausgehender Aufzählung) durchzuführen, da es am einfachsten umsetzbar ist.

Konkrete Umsetzung am Beispiel einer Hardwaregruppe mit Fujitsu-Netbooks
Zuerst muss vor dem Hochladen der Treiber ein Verzeichnis erstellt werden, in das die Treiber übertragen werden. Das Verzeichnis wird unter */var/lib/opsi/depot/opsi-local-image-win81-x64/drivers/drivers/additional* angelegt. Die Anlage des Verzeichnisses geschieht an der Konsole des Backup-Servers.

```
#cd /var/lib/opsi/depot/opsi-local-image-win81-x64/drivers/drivers/additional
#mkdir FutjitsuStylisticQ702
```

```
root@backup: /var/lib/opsi/depot/opsi-local-image-win81-x64/drivers/drivers/additional
root@backup:/var/lib/opsi/depot/opsi-local-image-win81-x64/drivers/drivers/additional# ls
byAudit
root@backup:/var/lib/opsi/depot/opsi-local-image-win81-x64/drivers/drivers/additional# mkdir FujitsuStylisticQ702
```

Abb. 148: Anlegen eines neuen Verzeichnisses für die Hardwaretreiber

Anschließend werden die Treiber in das soeben erstellte Verzeichnis auf den Backup-Server geladen.

Wenn Sie (wie oben beschrieben) die Hardwarekomponenten kennen, können Sie die zugehörigen Treiber zusammensuchen. Benötigt werden die **.inf*-Dateien. Ausführbare Archive (**.exe* oder **.msi*) sind nicht brauchbar, außer es handelt sich um selbst entpackende Archive, in denen die Treiber im **.inf*-Format vorliegen. Alle Archive müssen entpackt und die Inhalte auf den Server übertragen werden.

Der Einfachheit halber können die gesamten Inhalte von Archiven auf den Server übertragen werden. In der Praxis sollten Sie aber darauf achten, dass die richtigen Treiber in die richtigen Verzeichnisse gelangen. Das Hochladen der Treiber auf den Backup-Server geschieht zum Beispiel mit WinSCP (vgl. Kapitel 1.4.3 auf Seite 33).

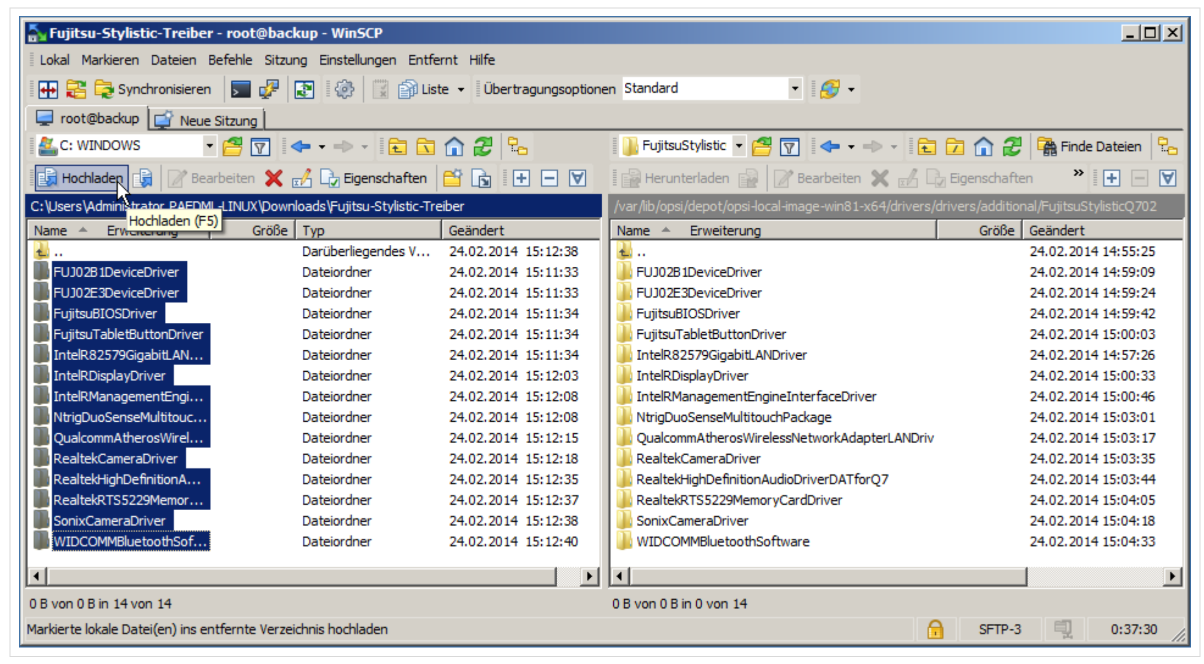


Abb. 149: Hochladen der Hardwaretreiber mit WinSCP



Damit *opsi* die neu auf den Server geladenen Dateien verarbeiten kann, muss der Befehl

```
#opsi-set-rights VERZEICHNISNAME
```

ausgeführt werden. Ersetzen Sie *VERZEICHNISNAME* durch den Namen des von Ihnen erstellten Verzeichnisses, in das die Treiber hochgeladen wurden.

```
root@backup: /var/lib/opsi/depot/opsi-local-image-win81-x64/drivers/drivers/additional
root@backup:/var/lib/opsi/depot/opsi-local-image-win81-x64/drivers/drivers/additional# ls
byAudit  FujitsuStylisticQ702
root@backup:/var/lib/opsi/depot/opsi-local-image-win81-x64/drivers/drivers/additional# opsi-set-rights FujitsuStylisticQ702/
[5] [Feb 24 15:16:24] Setting rights (opsi-setup|553)
[5] [Feb 24 15:16:25] Getting current system config (opsi-setup|126)
[5] [Feb 24 15:16:25] System information: (opsi-setup|179)
[5] [Feb 24 15:16:25]    distributor  : Univention (opsi-setup|180)
[5] [Feb 24 15:16:25]    distribution : Univention Corporate Server 3.2-1 errata62 (Borgfeld) (opsi-setup|181)
[5] [Feb 24 15:16:25]    ip address   : 10.1.0.2 (opsi-setup|182)
[5] [Feb 24 15:16:25]    netmask      : 255.255.255.0 (opsi-setup|183)
[5] [Feb 24 15:16:25]    subnet       : 10.1.0.0 (opsi-setup|184)
[5] [Feb 24 15:16:25]    broadcast    : 10.1.0.255 (opsi-setup|185)
[5] [Feb 24 15:16:25]    fqdn         : backup.paedml-linux.lokal (opsi-setup|186)
[5] [Feb 24 15:16:25]    hostname     : backup (opsi-setup|187)
[5] [Feb 24 15:16:25]    domain       : paedml-linux.lokal (opsi-setup|188)
[5] [Feb 24 15:16:25]    win domain   : PAEDML-LINUX (opsi-setup|189)
[5] [Feb 24 15:16:25] Setting rights on directory '/var/lib/opsi/depot/opsi-local-image-win81-x64/drivers/drivers/additional/
FujitsuStylisticQ702' (opsi-setup|637)
[5] [Feb 24 15:16:25] Setting rights on directory '/var/lib/opsi/depot/opsi-local-image-win81-x64/drivers/drivers/additional/
FujitsuStylisticQ702' (opsi-setup|637)
root@backup:/var/lib/opsi/depot/opsi-local-image-win81-x64/drivers/drivers/additional#
```

Abb. 150: Ausführen von opsi-set-rights

Der letzte auf dem Server durchzuführende Schritt ist das Setzen von Symlinks für opsi. Dies geschieht aus dem jeweiligen Haupt-Verzeichnis des betroffenen Netboot-Produktes (*/var/lib/opsi/depot/opsi-local-image-BETRIEBSSYSTEM*) mit dem Befehl

```
#./create_driver_links.py
```

```
root@backup: /var/lib/opsi/depot/opsi-local-image-win81-x64
root@backup:/var/lib/opsi/depot/opsi-local-image-win81-x64# ./create_driver_links.py
```

Abb. 151: Setzen von opsi-Symlinks.

Hiermit sind die Vorbereitungen auf dem Server abgeschlossen und die Treiberintegration in der *opsi*-Konsole kann vorgenommen werden.

7.7.3 Integration der Treiber in die Installation

Um den soeben im System hinterlegten Treiber bei der Installation einzubinden, markieren Sie im Auswahlfenster (4) der opsi-Konsole die zu installierenden Rechner.

Wählen Sie im Hauptfenster (5) den Reiter „*Netboot-Produkte*“ und dort das zu installierende Produkt. Tragen Sie im Feld „*Property-Wert*“ von „*additional_drivers*“ den Namen des von Ihnen erstellten Verzeichnisses, in dem die Treiberdateien liegen, ein. Der Verzeichnis-Name ist dabei ohne den Verzeichnis-Pfad anzugeben (vgl. folgender Screenshot). Speichern Sie die Änderungen.



Der Wert des Verzeichnisnamens ist case-sensitive. Es ist also wichtig, dass Sie den genauen Namen (Groß-/Kleinschreibung beachten) eintragen!

Konfiguration für Client

Property-Name	Property-Wert
additional_drivers	FujitsuStylisticQ702
askbeforeinst	False
backup_after_install	False
fullname	Name
imagename	Windows 8.1 Pro
orgname	Orgname

Abb. 152: Eintrag des Verzeichnisnamens der Treiberdateien

Anschließend können Sie (bevorzugt mit dem *Netbootprodukt „opsi-local-image-prepare*“) die Installation starten.

7.8 Troubleshooting – Probleme beim Booten

7.8.1 Konfigurieren von Bootparametern

opsi bootet beim Systemstart über das Netzwerk ein Mini-Linux, das Aufgaben, wie das Ausspielen von *Netboot-Produkten* übernimmt. Dieses Mini-Linux bekommt in regelmäßigen Abständen Updates, so dass der Kernel, den *opsi* verwendet, stets relativ aktuell ist.

Aufgrund der Heterogenität von Hardware kann es dennoch zu Problemen beim Starten eines Rechnermodells geben. Hier können Sie versuchen, die Bootparameter der betroffenen Rechner anzupassen. Markieren Sie hierfür den (oder die) Rechner in der Übersicht (4). Wechseln Sie in den Reiter „*Hostparameter*" und öffnen Sie den ersten Eintrag (ohne Bezeichnung).

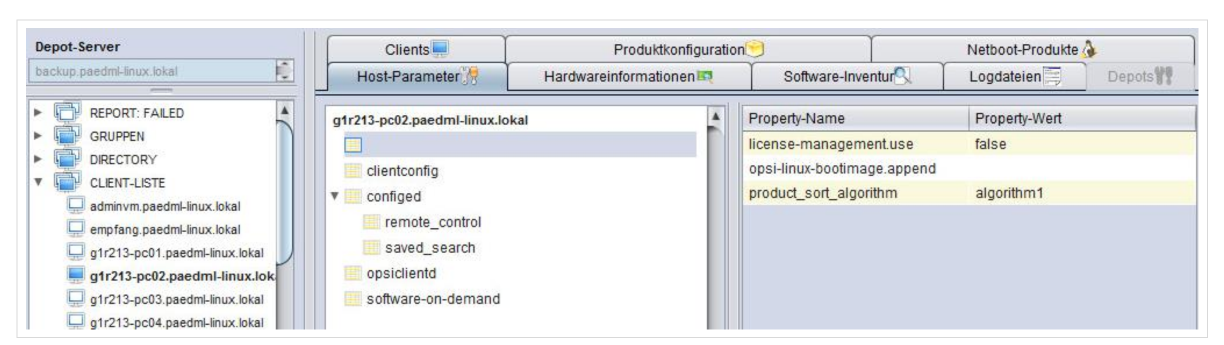


Abb. 153: Anpassen von Hostparametern für den Systemstart.

Im dynamisch gefüllten Bereich der *opsi*-Konsole (6) gibt es den Parameter „*opsi-linux-bootimage.append*", an dem Anpassungen vorgenommen werden können. Um mehrere Werte auszuwählen, drücken Sie bitte die Strg-Taste und wählen Sie mit der linken Maustaste die Einträge, die in das Feld „*Property-Wert*" übernommen werden sollen.

Speichern Sie die Werte, bevor Sie die Maske schließen.

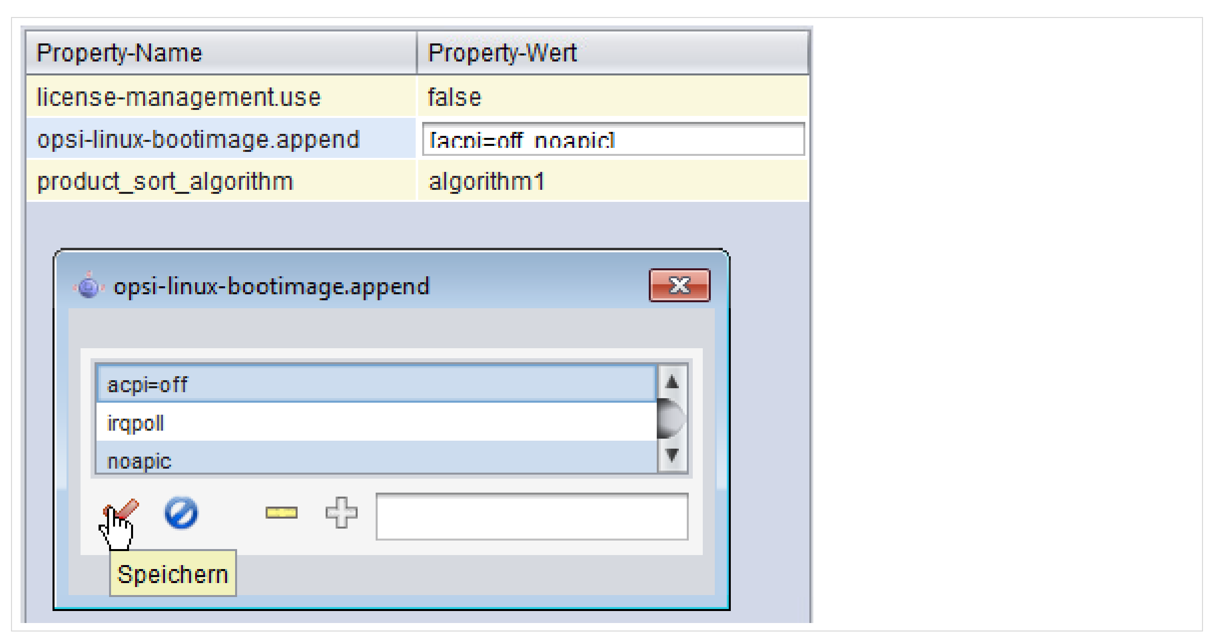


Abb. 154: Eintrag von Bootparametern in opsi

Zusätzlich zu den Anpassungen in *opsi* müssen Sie ggf. die Einstellungen des BIOS der betroffenen Rechner überprüfen und ändern.

Hierbei handelt es sich um Festplattenparameter des BIOS. Bezeichnungen und verfügbare Werte variieren je nach Hersteller:

- *SATA: deaktiviert, auto, IDE, Native, Legacy*
- *AHCI: aktiviert, deaktiviert*

- *LBA: aktiviert, deaktiviert, auto*
- *32-Bit-Zugriff: aktiviert, deaktiviert*

Bei problematischer Hardware wird man es nicht vermeiden können, durch systematisches Probieren eine funktionierende Kombination aus PXE- und BIOS-Einstellungen zu finden.

7.8.2 Anzeige der opsi-Konsolenausgabe im Fehlerfall

Sollte sich Hardware partout nicht booten lassen, kann möglicherweise ein Blick in die Ausgabe des Bootvorganges von *opsi* weiter helfen. Diese Ausgabe verbirgt sich in der Standardkonfiguration hinter einem Splash-Screen und kann erst nach Anpassungen sichtbar gemacht werden.

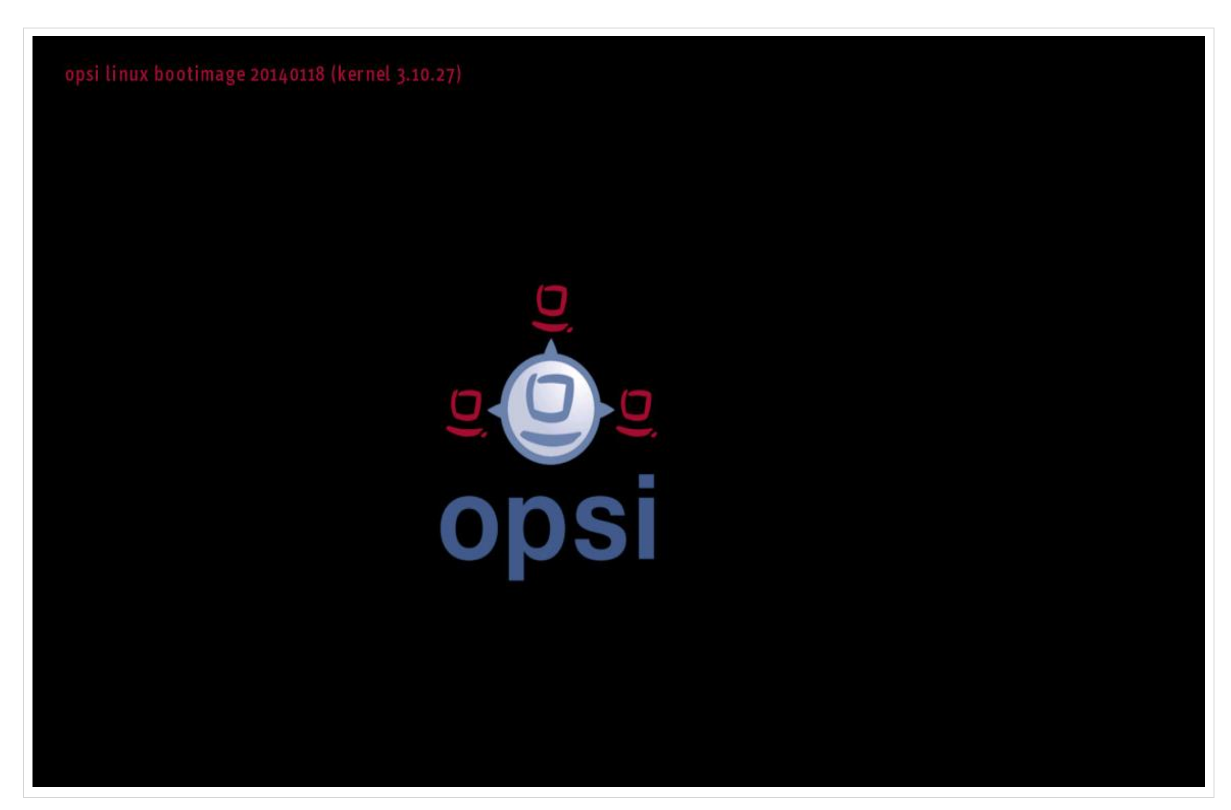


Abb. 155: Standard Splash-Screen

Um das *opsi*-Logo auszublenden, müssen Sie die Datei */tftpboot/linux/pxelinux.cfg/install* bearbeiten.

Entfernen Sie die letzten beiden Wörter „*quiet*“ und „*splash*“. Erstellen Sie vor dem Ändern eine Sicherungskopie der Originaldatei!

Originaldatei:

```
default opsi-install

label opsi-install
  kernel install
  append initrd=miniroot.bz2 video=vesa:ywrap,mtrr vga=791 quiet splash
```

geänderte Version:

```
default opsi-install

label opsi-install
  kernel install
  append initrd=miniroot.bz2 video=vesa:ywrap,mtrr vga=791
```

Wenn Sie anschließend einen Rechner starten, wird das *opsi*-Logo nicht mehr angezeigt. Stattdessen werden auf dem Bildschirm die Meldungen des Systemboots ausgegeben. Aus der Anzeige der Boot-Meldungen können Fehler ausgelesen werden.

7.8.3 Log-Dateien zu Boot-Problemen

Sollte das Problem auch über die Ausgabe des *opsi*-Bootimages nicht erkennbar sein, hilft häufig ein Blick in die Log-Datei des Rechners.

Beim Start von Clients schreibt *opsi* Logdateien, die – sofern der Rechner eine Netzwerk-Verbindung hat – auf dem Backup-Server unter */var/log/opsi/bootimage* abgelegt werden. Hier wird für jeden Client eine Datei erstellt.

Sollte der Rechner beim Starten den Backup-Server nicht erreichen und keine Log-Datei übertragen können, so findet sich die Logdatei im Bootimage unter */tmp/log/*. Um in einem solchen Fall an die Logdatei des Bootimages zu kommen, gibt es zwei Wege:

5. Wenn der Rechner eine Netzwerkverbindung hat, kann man per WinSCP die Datei /tmp/log vom Client holen.
6. Wenn das Netzwerk vom Client aus nicht erreichbar ist, können Sie die Datei per USB-Stick übertragen. Loggen Sie sich hierfür auf dem Client an der Linux-Konsole ein:
   `Benutzername root, Kennwort linux123`
   Verbinden Sie einen USB-Stick mit dem Rechner und warten Sie ein paar Sekunden. Mit dem Befehl `sfdisk -l` prüfen Sie, auf welchem Device der USB-Stick eingebunden wurde.
   Anschließend muss der USB-Stick eingebunden (`#mount`), die Datei kopiert und der USB-Stick wieder ausgehängt werden.
   Anschließend können Sie die Logdatei für die Analyse auslesen oder der Hotline senden. Selbstverständlich kann die Log-Datei auch lokal ausgelesen werden.

Ein Beispiel für dieses Verfahren.

```
#sfdisk -l
Disk /dev/sda: 30401 cylinders, 255 heads, 63 sectors/track
Units = cylinders of 8225280 bytes, blocks of 1024 bytes, counting from 0
Device           Boot   Start  End    #cyls #blocks           Id     System
/dev/sda1   *      0+     30401  30402  244197528    7      HPFS/NTFS
/dev/sda2          0      -      0      0            0      Empty
/dev/sda3          0      -      0      0            0      Empty
/dev/sda4          0      -      0      0            0      Empty

Disk /dev/sdb: 1017 cylinders, 33 heads, 61 sectors/track
Units = cylinders of 1030656 bytes, blocks of 1024 bytes, counting from 0
Device           Boot   Start  End    #cyls #blocks           Id     System
/dev/sdb1          0+     1016   1017-  1023580      b      W95 FAT32
/dev/sdb2          0      -      0      0            0      Empty
/dev/sdb3          0      -      0      0            0      Empty
/dev/sdb4          0      -      0      0            0      Empty
# mount /dev/sdb1 /mnt
# cp /tmp/log /mnt
#umount /mnt
```

7.9 Einspielen von Software



Wenn der zu installierende Rechner bereits über *opsi* verwaltet und das Betriebssystem erneut installiert wurde, sind in der Datenbank von *opsi* noch alte Informationen zu der bisher installierten Software eingetragen. Diese Werte müssen manuell gelöscht werden!

Um die Informationen zu löschen, müssen Sie den neu installierten Rechner in der *Clientliste* (4) markieren. Anschließend öffnen Sie in der *Menüleiste* (1) den Eintrag „*opsiClient* | *Localboot-Produkte zurücksetzen*“. Im anschließenden Dialogfenster müssen Sie die Änderungen mit „*Ja*“ übernehmen.

Die Werte in der „*Produktkonfiguration*“ des Rechners sind anschließend unwiederbringlich gelöscht.

Bei der Softwareverteilung kommen die *Localboot-Produkte* zum Einsatz. Um Software auszuspielen, öffnen Sie im Hauptfenster (5) den Reiter „*Produktkonfiguration*“.

Software, die Sie auf Clients ausspielen wollen, muss im *opsi-Depot* vorgehalten werden. Wie Sie Software in das *opsi-Depot* hoch laden können, ist in Kapitel 7.13 auf Seite 157 beschrieben.

Die Verteilung eines *Localboot-Produktes* kann auf einzelne Rechner oder auf Rechnergruppen geschehen, die in der Rechnerliste (4) markiert wurden.

Wählen Sie das Produkt aus und klicken Sie in die Spalte „*Angefordert*“. Wählen Sie dort den Eintrag „*Setup*“.

Der dynamische Inhalt der *opsi*-Konsole (6) wird nun mit Informationen zum ausgewählten Produkt und mit Parametern („*Konfiguration für Client*“) gefüllt, die angepasst werden können. Wenn Abhängigkeiten zu anderen Paketen bestehen, werden diese aufgelöst. Im folgenden Screenshot benötigt *Libre Office* ein Paket namens *javavm*, das automatisch auf dem Client mitinstalliert wird, sobald das Paket „*libreoffice*“ für die Installation ausgewählt wurde.

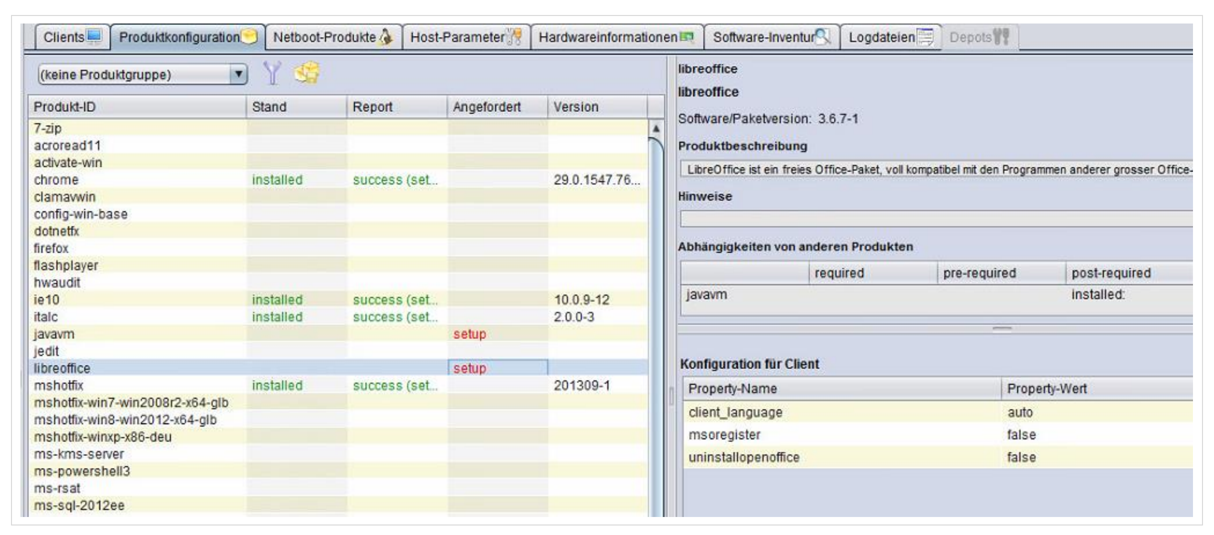


Abb. 156: Softwareinstallation am Beispiel von Libreoffice

Alle Änderungen müssen anschließend wieder mit dem *roten Haken* unter (2) gespeichert werden.

Sie können die Installation von *Produktpaketen* entweder gleich nach der Konfiguration von *Netboot-Produkten*, also wenn noch kein Betriebssystem vorhanden ist, vornehmen. Die Software wird im Anschluss an die Installation des Betriebssystems ausgespielt.

Oder Sie können nachträglich Programme auf installierten Rechnern ausspielen.

Die Installation der ausgewählten *Netboot-Produkte* startet automatisch, wenn der Rechner das nächste Mal hochgefahren wird. *opsi* überprüft nach jedem Systemstart, ob es Aktualisierungen für den Rechner gibt.

Alternativ kann die Installation neuer Pakete manuell ausgelöst werden. Um die Installation auszulösen, wechseln Sie im Hauptfenster (5) in den Reiter *Clients* und klicken Sie mit der rechten Maustaste über die ausgewählten Clients. Sie haben nun verschiedene Optionen, um die Installation zu initiieren. So können Sie – sofern der Rechner das unterstützt – bei ausgeschaltetem System einen Systemstart anstoßen. Sie können bei eingeschalteten Rechnern auch ein *Ereignis ‚on_demand'* auf den ausgewählten Clients auslösen.

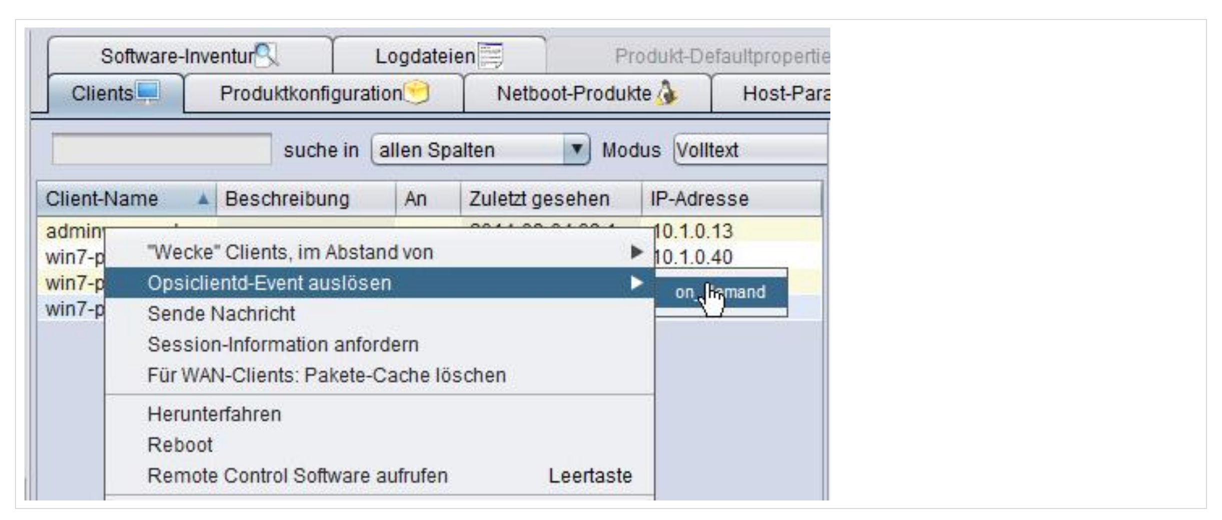


Abb. 157: Start der Softwareinstallation

7.10 Empfohlene opsi-Localboot-Produkte



Wenn die Rechner für die automatische Installation markiert sind (vgl. Kapitel 7.5.1, Seite 135), wird automatisch Software installiert. Darin enthalten sind unter anderem das Paket für den Domänenbeitritt, die Software *italc*, die für die Fernsteuerung über die Schulkonsole benötigt wird und andere Softwarepakete.

Wenn ein Rechner manuell mit Software versorgt wird, so gibt es einige Pakete, die installiert werden müssen, damit die Funktionen der *paedML Linux* im pädagogischen Netzwerk gewährleistet sind. **Bitte wählen Sie diese nachfolgend genannten Pakete unbedingt aus!** (Fast)[41] alle hier beschriebenen *Netboot-Produkte* und weitere Programme finden Sie im *opsi*-Paket *„clientprodukte"*, das bei der automatischen Rechnerinstallation aktiv ist oder manuell ausgespielt werden kann.

1. *Windomain* – Dieses Paket führt den Domänenbeitritt der Rechner durch und muss installiert werden. Bei jeder Wiederherstellung eines Images (siehe Kapitel 9.3 auf Seite 170) wird dieses Paket ausgeführt, um dem Rechner erneut in die Domäne aufzunehmen.
2. *italc* – Dieses Paket ermöglicht den Zugriff auf Schülerrechner aus der *Schulkonsole*. Die Funktionsweise ist im Lehrerhandbuch beschrieben.
3. *google-chrome-for-business* – Wir empfehlen *Chrome* als Standardbrowser für die *paedML Linux*. Sie können auch andere Browser verwenden. Es treten aber unter Umständen Probleme auf, beispielsweise beim Umgang mit Server-Zertifikaten.
4. *zertifikat* – Dieses Paket installiert das Stammzertifikat des Servers, das für die verschlüsselte Kommunikation zwischen Server und Clients (z.B. *Schulkonsole*, …) benutzt wird.
5. *config-win-base* – Dieses Paket nimmt einige Einstellungen unter *Windows* vor.
6. *usbdim* – verhindert, dass sich USB-Laufwerke (z.B. Cardreader) von der *paedML* reservierte Laufwerksbuchstaben (z.B. *H:*\) übernehmen.
7. *shutdownwanted* – Über dieses Paket können Rechner nach der Durchführung von Installationen automatisiert heruntergefahren werden. Dieses Paket ist nötig, da *opsi* Rechner so lange neu startet, bis keine Aktionen mehr ausgeführt werden. Ein Rechner würde also ohne dieses Paket nach der Installation eingeschaltet bleiben.
8. Des Weiteren empfehlen wir Ihnen, alle in *opsi* verfügbaren *Hotfixes* auszuspielen.

7.11 Neuinstallation von Rechnern



Dieses Kapitel ist nur dann relevant, wenn Sie Rechner neu aufsetzen und mit abweichender Software installieren wollen.

opsi speichert alle Informationen über verwaltete Rechner in einer Datenbank. Hier werden auch alle über *opsi* auf dem Rechner installierten Programme hinterlegt.

Wenn die Installationsdaten von Rechnern nicht – wie hier beschrieben – bereinigt

[41] Das Paket windomain ist nicht im Paket „clientprodukte" enthalten, da der Domänenbeitritt über einen anderen Automatismus angestoßen wird.

werden, spielt *opsi* automatisch nach der Installation des Betriebssystems die für den Rechner hinterlegten Programme ein.

Vor einer kompletten Neuinstallation von Rechnern, die mit *opsi* verwaltet werden, sollte der Datensatz der betroffenen Geräte bereinigt werden.,Alle Informationen zu *Localboot-Produkten* – also der von *opsi* installierten Software - der vorherigen *Windows*-Installation müssen hierbei gelöscht werden.

Um die *opsi*-Datenbank zu bereinigen, öffnen Sie zunächst den *opsi-configed,* wechseln Sie dann in die Rechner-Liste im Reiter *„Clients“* und markieren Sie die Rechner, deren Informationen über installierte *Localboot-Produkte* gelöscht werden sollen.

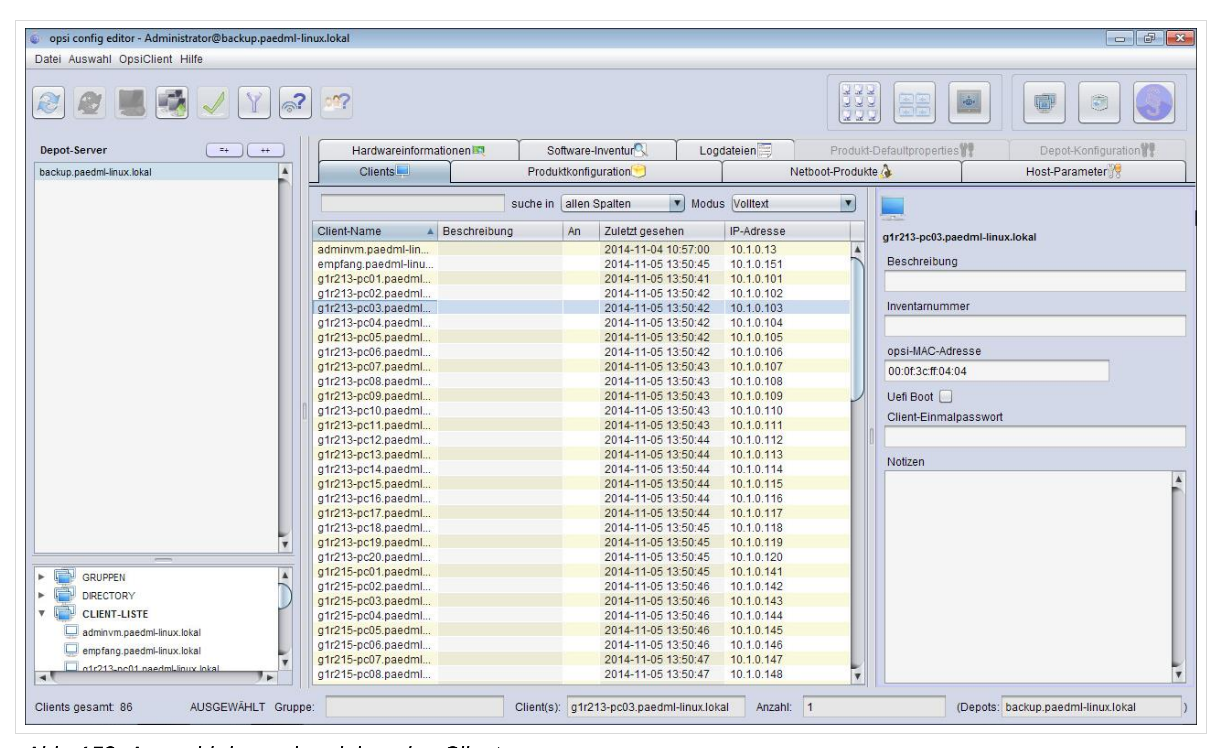


Abb. 158: Auswahl des zu bereinigenden Clients

Ein Klick auf die ausgewählten Rechner mit der rechten Maustaste öffnet ein Menü. Dort müssen Sie den Eintrag "*Localboot-Produkte zurücksetzen*" auswählen.

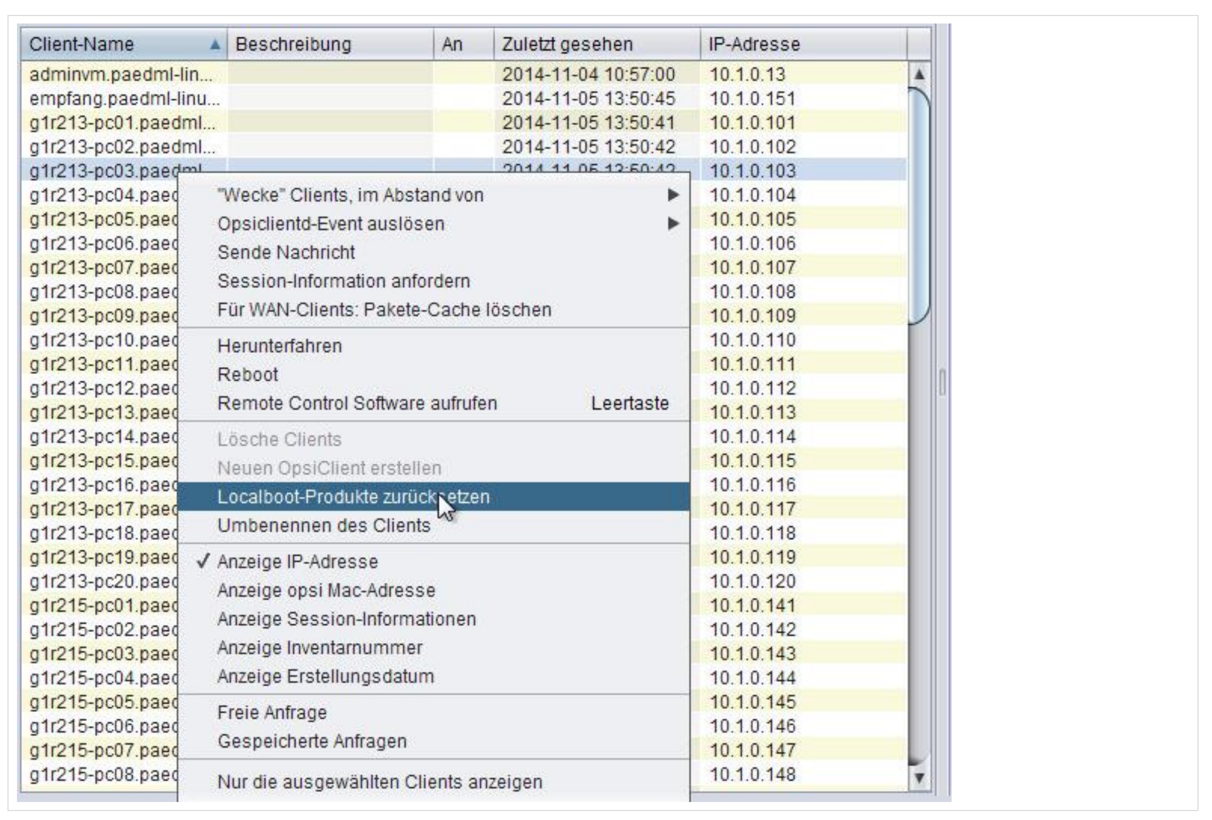


Abb. 159: „Localboot-Produkte zurücksetzen

Nun werden alle den Rechnern zugeordneten *Localboot-Produkte* aus der Datenbank gelöscht und *Windows* kann auf die Rechner neu ausgerollt werden.

7.12 Erstellen von opsi-Paketen

Das Erstellen von *opsi*-Paketen ist Aufgabe eines Dienstleisters.

Nähere Informationen zum Erstellen von *opsi*-Paketen entnehmen Sie dem opsi-Handbuch http://download.uib.de/opsi4.0/doc/html/opsi-getting-started/opsi-getting-started.html#opsi-getting-started-softwintegration .



Die Erstellung, Einrichtung und Problembehandlung von *opsi-Paketen*, die nicht von Servern des Landesmedienzentrums bezogen werden, wird nicht durch die Mitarbeiter des *Support-Netzes* unterstützt.

7.13 Einbindung von opsi-Paketen

Alle Programme, die über *opsi* verteilt werden können, liegen auf dem Backup-Server im Verzeichnis */var/lib/opsi/depot/PROGRAMMNAME* .

Unter */var/lib/opsi/depot/* finden Sie alle *opsi*-Produkte, also Localboot-Produkte wie Programme (z.B. der Editor *jedit*) und Netboot-Produkte, die für die Installation benötigt werden (z.B. opsi-local-image-win8.1-x64).

opsi-Pakete können verschiedene Quellen haben:

- Die *paedML Linux* wird mit einigen *opsi*-Paketen ausgeliefert. Das *Support-Netz* stellt hierzu auf einem Updateserver Aktualisierungen zur Verfügung, die automatisch heruntergeladen und in das *opsi*-Depot aktualisiert werden. Das Angebot kann sich mit der Zeit ändern!
- Daneben können Inhalte aus anderen Quellen manuell eingebunden werden (z.B. Angebote der *SoN*-Gruppe). Diese Software muss in das *opsi*-Depot übertragen werden. Aktualisierungen müssen manuell vorgenommen werden.
- Darüber hinaus können Sie Dienstleister beauftragen, um Software für *opsi* zu paketieren oder eigene Pakete schnüren. Ein Dienstleister wäre die Firma *uib* (www.uib.de), die *opsi* entwickelt.
- Es gibt im Internet auch Paketquellen von *opsi*-Paketen. Informationen hierzu finden Sie unter anderem hier: https://forum.opsi.org/wiki/userspace:packaging_links



Achtung! Das Ausspielen von *opsi*-Paketen von Drittanbietern geschieht ausdrücklich auf eigene Gefahr.

opsi-configed führt Sie mit dem Knopf „*Produktverwaltung*" in ein Dialogfenster, über das Sie *opsi-Pakete* installieren können. Sie können über diese Funktion *Localboot-Pakete* auf den Server laden. Sie finden den Knopf oben rechts in der *opsi*-Mangement-Konsole.



Abb. 160: Der Button „Produktverwaltung"

Um ein *opsi-Paket* in das System einzuspielen, müssen Sie eine *.opsi-Datei* vorliegen haben. In diesem Beispiel wurde die Datei *gimp_2.8.0-2.opsi* aus dem Internet heruntergeladen und installiert.

Das sich öffnende Dialogfenster ist wie folgt aufgebaut:

Im oberen Feld "*opsi Paket-Installation*" werden neue Programmpakete in *opsi* eingespielt. Das untere Feld „*Vervollständigung eines Windowsprodukts*" ist für das Einspielen der *Netboot-Produkte* (vgl. Kapitel 7.4.1, Seite 131).

Im ersten Feld „*opsi-Paket*" wird der Speicherort der *.opsi-Datei* eingetragen. Das blaue Ordnersymbol öffnet einen Filebrowser, mit dem Sie zum Speicherort der Datei navigieren können.

Der Wert für „*Installieren auf*" ist mit dem Namen des *opsi-Servers* (backup.paedml-linux.lokal) vorbelegt.



Damit Sie auf das *opsi-Depot* zugreifen können, müssen Sie an dem Arbeitsplatz, von dem aus Sie Änderungen vornehmen, als **Administrator der Domäne** angemeldet sein.

Die nächste Zeile zeigt an, ob Sie mit dem opsi-Workbench verbunden sind und Dateien auf den *opsi-Server* hochladen können.

Der Eintrag „*(Anderes) Zielverzeichnis*" ist ebenfalls vorbelegt und kann nicht geändert werden.

Mit einem Klick auf das Symbol mit dem gelben Stern („*Paketinstallation durchführen*") laden Sie das *opsi-Paket* auf den *opsi-Server*.

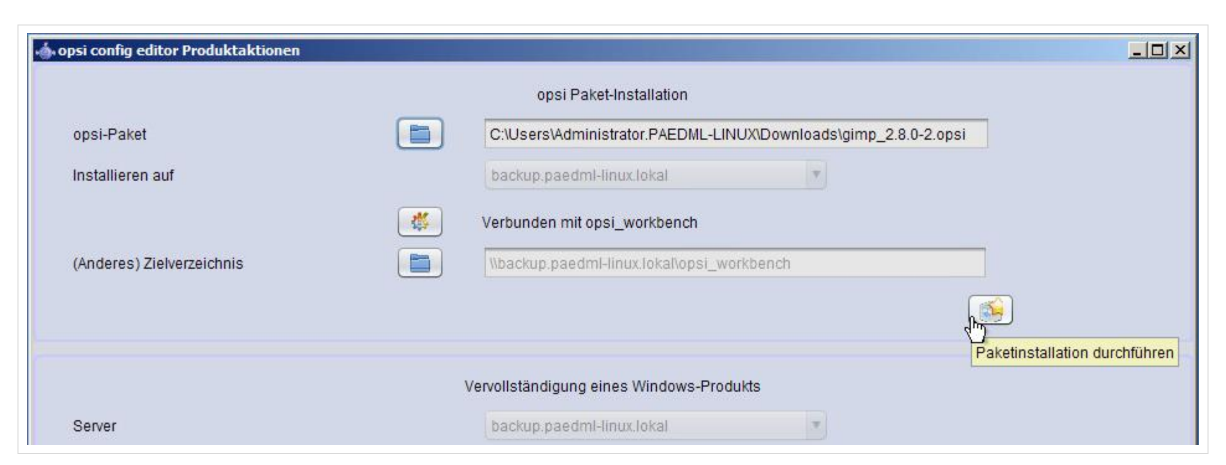


Abb. 161: Einspielen eines opsi-Paketes

Anschließend können Sie das neu eingespielte Paket im Schulnetz verteilen. Damit das Paket im Reiter „*Produktkonfiguration*" im Hauptfenster (5) angezeigt wird, muss der Datensatz von *opsi* neu eingelesen werden. Dies geschieht über die beiden blauen Pfeile im Schnellzugriffsmenü (2) oben links.

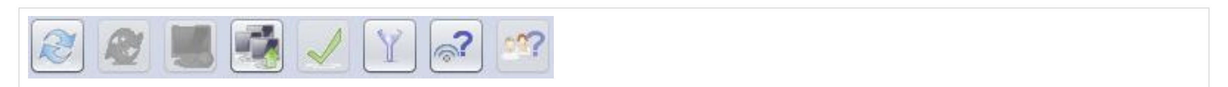


Abb. 162: opsi-Schnellzugriffsmenü – mit dem Symbol ganz links werden die opsi-Informationen neu geladen

7.14 Bearbeitung ganzer PC-Räume

Um ganze Rechnergruppen wiederherzustellen, müssen Sie mehrere Clients in der Clientliste markieren. Im Anschluss können Sie mit den *opsi*-Produkten wie oben beschrieben arbeiten. Sie können auf diesem Weg auch Software an mehrere Rechner verteilen.

Dies bedeutet, dass Sie bequem an der *opsi*-Konsole viele Rechner zeitgleich mit Betriebssystem und Software versorgen können. Sie können auf demselben Weg alle Rechner in die jeweilige Backuppartition sichern und wiederherstellen.

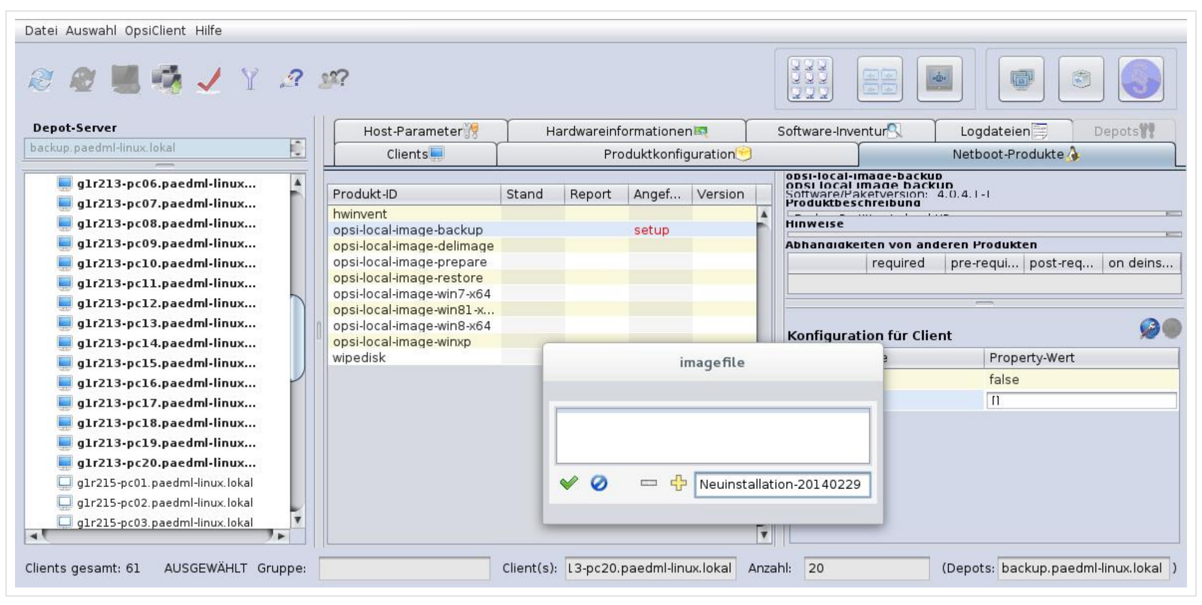


Abb. 163: Verwaltung mehrerer Rechner mit der opsi-Konsole..

7.14.1 Arbeiten mit Gruppen

Sie können – wie soeben beschrieben – mehrere Computer über die Client-Liste markieren oder über den Knopf „*Gruppen*“ in der Rechnerliste (4) auswählen. Hierbei können Sie – sofern Computerräume in der Schulkonsole definiert wurden (vgl. Kapitel 5, Seite 89) und die entsprechenden Rechner den Räumen zugewiesen sind – die Auswahl auf Rechner eines Raumes beschränken.

1. Markieren Sie bitte hierfür den Knopf „*Gruppen*“ und wählen Sie in der Liste (muss ggf. ausgeklappt werden) den Raum, der bearbeitet werden soll (im Beispiel der Raum „*schule-g1r315*“).
2. Anschließend wechseln Sie im Hauptfenster (5) in den Reiter „*Clients*“ und markieren Sie alle Rechner, die Sie konfigurieren wollen. Sie können auch hier mit der Strg-Taste einzelne Clients an- bzw. abwählen oder mit der Shift-Taste Bereiche selektieren.

   Die Rechner der Auswahl können nun über *opsi* mit Software versorgt werden.

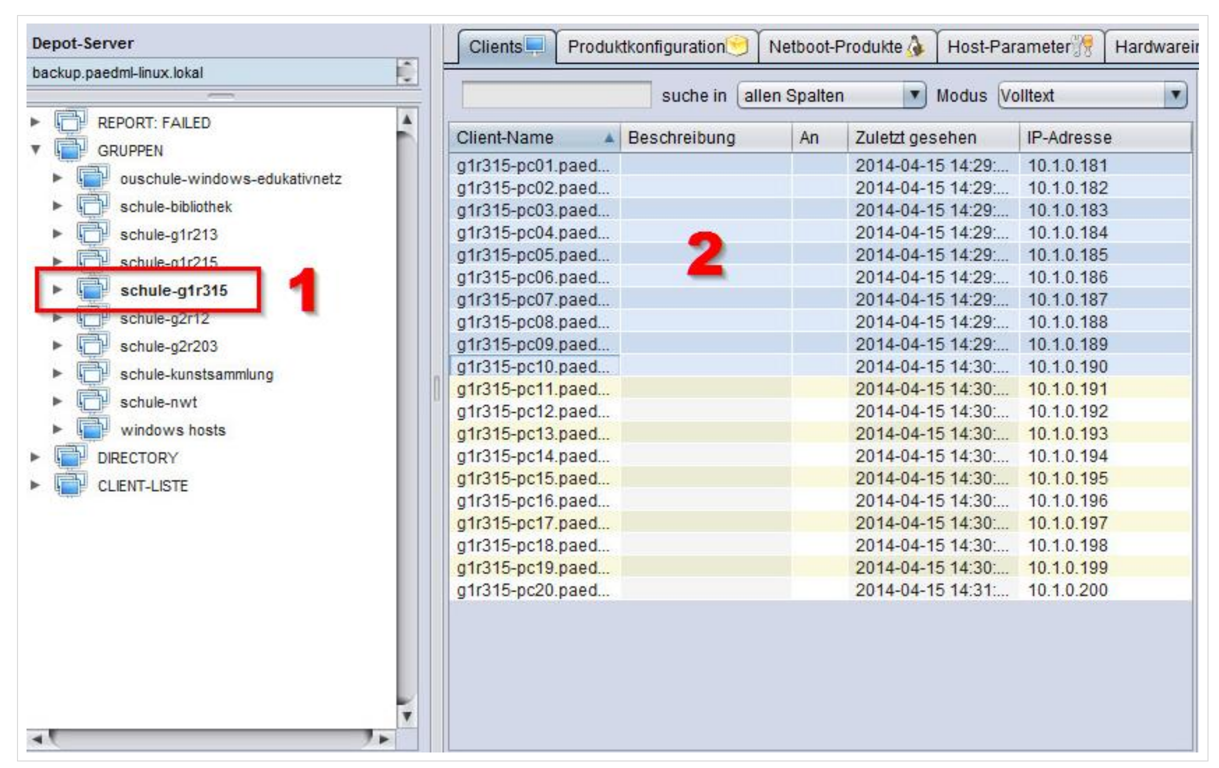


Abb. 164: Auswahl einer Rechnergruppe (entspricht Raum) (1) und darin befindlicher Clients (2)

8. Übernahme alter Rechner in die Domäne

Es kommt – vor allem bei der Einrichtung eines neuen Netzwerkes – immer wieder vor, dass bestehende Rechner(gruppen) ohne Anpassung am Image des Rechners in die neue Domäne übernommen werden sollen.

Die Integration bestehender Rechner erfolgt in drei Schritten:

1. Rechner in die *paedML* aufnehmen.
2. Ausspielen von *opsi-client-agent*
3. Rechner in die Domäne aufnehmen.



1. Rechner, die nicht mit *opsi* partitioniert wurden, können nicht mit *opsi-local-image-Paketen* versorgt werden. Dies bedeutet, dass (mittels *opsi*) keine Images erstellt und zurück gespielt werden können.
2. Unter *opsi* sind keine Informationen darüber verfügbar, welche Software auf dem Client installiert wurde. Nur Programme, die über *opsi* verteilt werden sind in der *opsi*-Maske als installiert sichtbar.

Wir empfehlen am Client das Paket „*clientprodukte*“ zu installieren.

8.1.1 Rechneraufnahme in die paedML

Zunächst müssen Sie den Rechner (wie in Kapitel 4 Verwaltung von Geräten, Seite 48 beschrieben) in die neue *paedML* aufnehmen. Bei der Rechneraufnahme muss der Rechnername des aufgenommenen Rechners (LDAP-Objekt) mit dem *Windows*-Rechnernamen übereinstimmen, ggf. muss vor der Aufnahme in die *paedML* der *Windows*-Rechnername an die Begebenheiten im Schulnetz angepasst werden.

Damit sind die Clients weder in die Domäne aufgenommen noch per *opsi* administrierbar. Um dies zu gewährleisten muss zunächst der *opsi-Client-Agent* installiert werden. Anschließend können Sie den Client in die Domäne aufnehmen.

8.1.2 Ausspielen von opsi-client-agent



Der opsi-client-agent muss immer (neu) installiert werden, wenn ein Rechner in eine neue Domäne aufgenommen wird. Dies gilt auch für Systeme, auf denen das Programm bereits installiert wurde.

Auf dem *opsi-Server* („*backup*“) finden Sie in der Netzwerkfreigabe *\\backup\opsi-depot\opsi-client-agent* das Skript „*service_setup.cmd*“, das auf dem Rechner, der mit *opsi* bekannt gemacht werden soll, ausgeführt werden muss.

Melden Sie sich an einem *Windows*-Rechner an, öffnen Sie über den *Windows-Explorer* die Freigabe (Zugangsdaten des Domänenadministrators) und führen Sie das Skript aus.

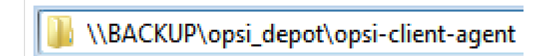


Abb. 165: *Eingabe des Pfades in einen* Windows-*Explorer*

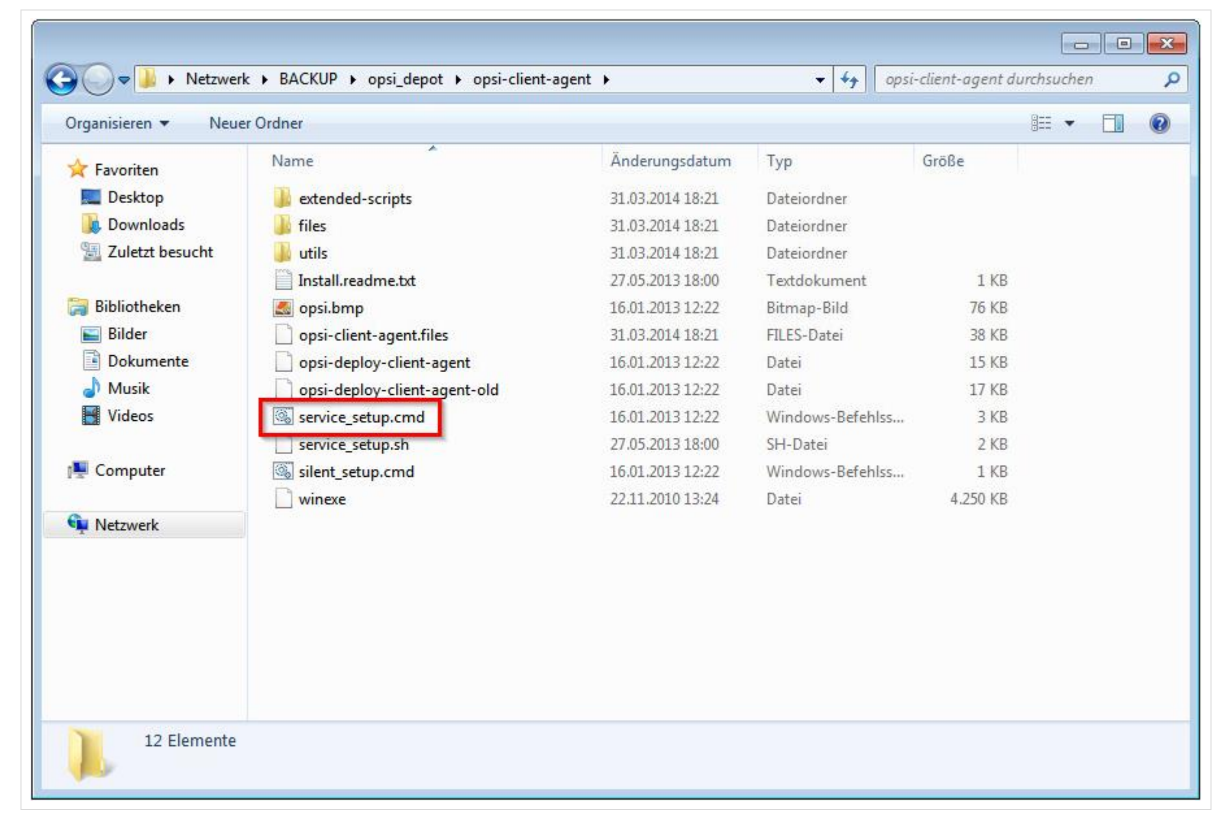


Abb. 166: Zugriff auf die Netzwerkfreigabe

Nach einem Doppelklick öffnet sich eine *Windows*-Konsole, in der Sie zur Bestätigung der Installation von „*opsi-client-agent*" auf dem lokalen Rechner aufgefordert werden.

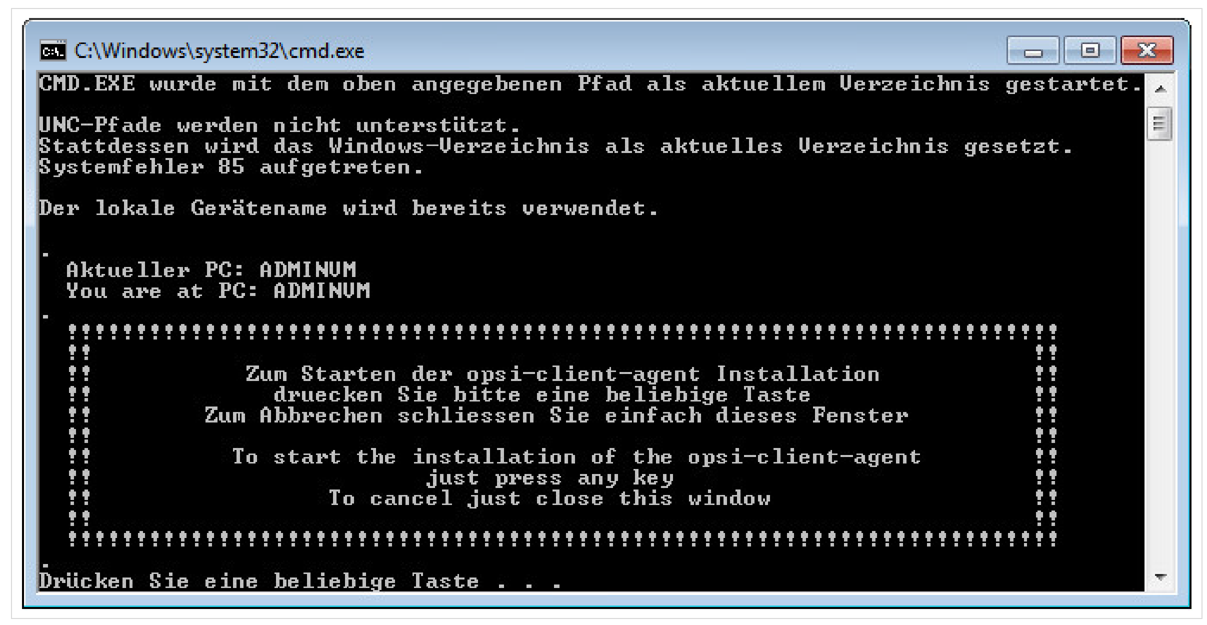


Abb. 167: Windows-*Konsole vor Installation*

Wenn Sie die Installation bestätigt haben, wird das Programm installiert.



Abb. 168: Installation von opsi-client-agent

Um die Installation vollständig auszuführen benötigt das Paket erneut die Eingabe der Zugangsdaten des Domänen-Administrators.

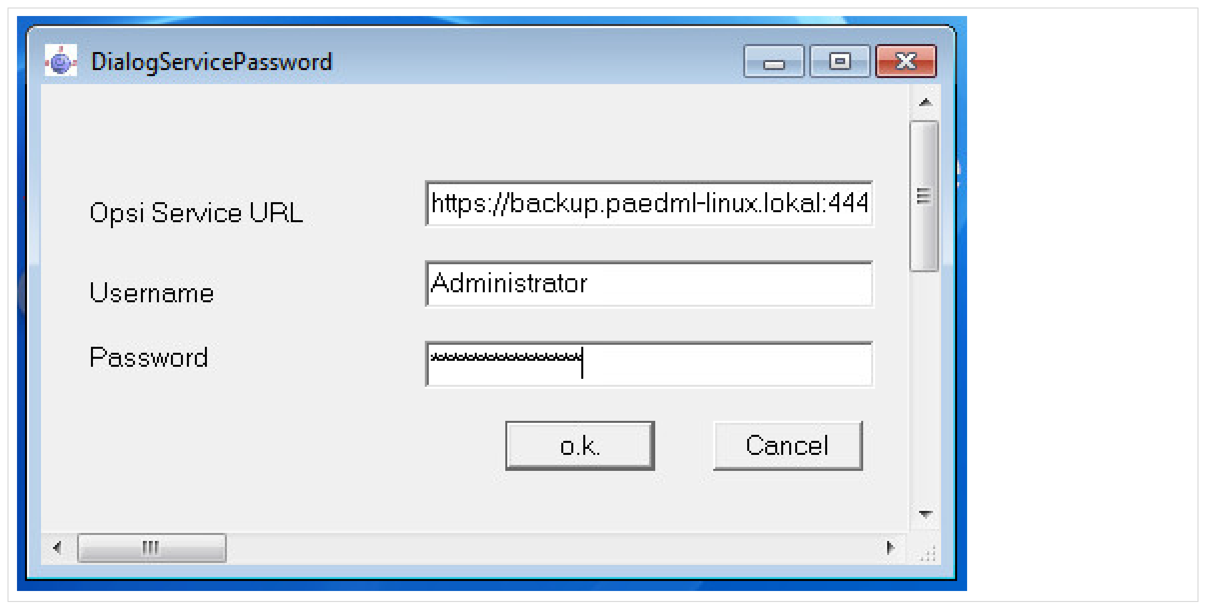


Abb. 169: Erneute Eingabe der Zugangsdaten von Domänenadministrator

8.1.3 Rechneraufnahme in die Domäne

Folgende Szenarien der Computeraufnahme in die Domäne sind möglich:

Variante 1 - Manuelle Aufnahme der Clients in die Domäne
Um einen Client manuell in die Domäne *paedml-linux.lokal* zu integrieren, müssen Sie sich als lokaler Administrator am Client anmelden.

Öffnen Sie die Systemsteuerung und dort den Menüpunkt „*System*". Im Abschnitt „*Einstellungen für Computernamen, Domäne und Arbeitsgruppe*" finden Sie den Eintrag „*Einstellungen ändern*" (1). Wenn Sie diesen Punkt ausgewählt haben, öffnet sich ein neues Fenster „*Systemeigenschaften*". Klicken Sie auf „*Ändern*" (2), um das nächste Dialogfenster „*Ändern des Computernamens bzw. der Domäne*" aufzurufen.

Hierin überprüfen Sie, ob der Computername mit dem Namen des Rechners in der paedML(vgl. Kapitel 8.1.1) übereinstimmt. Tragen Sie den Namen der Domäne „*paedml-linux.lokal*" in das hierfür vorgesehene Feld ein (3).

Sie werden für den Domänenbeitritt nach einem Benutzer und einem Kennwort gefragt. Es handelt sich hierbei um den Administrator der Domäne, oder dem domadmin.

Bestätigen Sie die Eingaben jeweils mit „OK" und führen Sie im Anschluss einen Neustart aus, damit die Änderungen übernommen werden.



Sollte der Computer Mitglied einer anderen Domäne gewesen sein, müssen Sie zunächst – analog dem hier vorgestellten Verfahren einer beliebigen Arbeitsgruppe beitreten und anschließend den Rechner neu starten, bevor Sie ihn schließlich in die Domäne „*paedml-linux.lokal*" aufnehmen können.

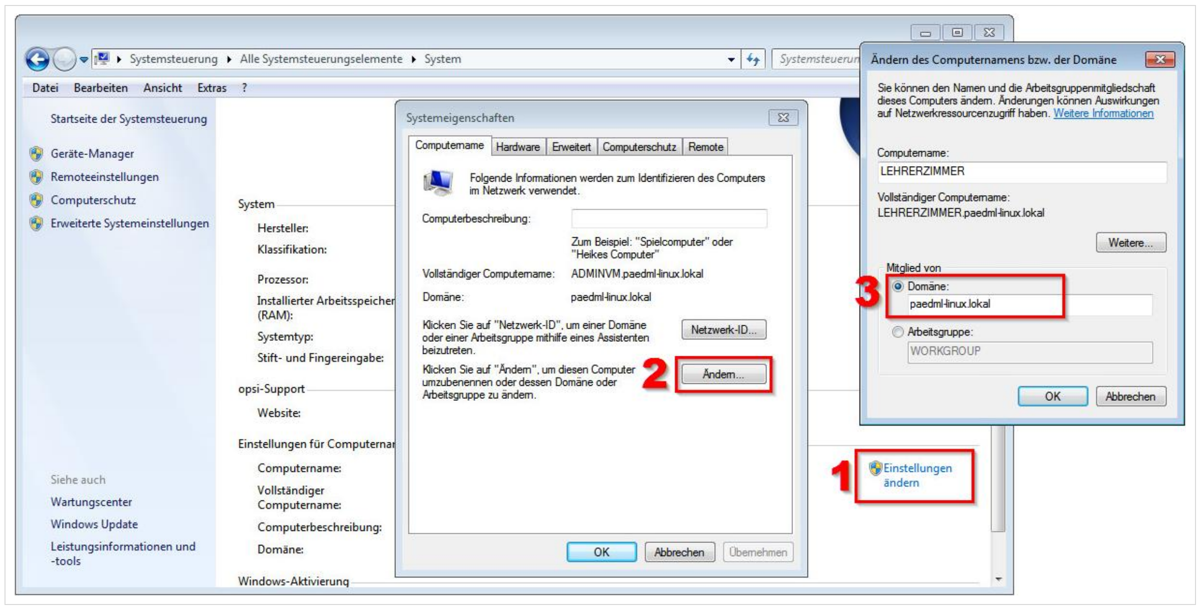


Abb. 170: Ändern der Domäne

Damit ist der Rechner in der Domäne aber noch nicht per *opsi* administrierbar. Hierfür müssen Sie den *opsi-client-agent* installieren (vgl. Kapitel 8.1.2).

Variante 2 - Domänenbeitritt über das *opsi*-Paket „*windomain*"
Für den neu in die paedML aufgenommen Client kann das Pakte „*windomain*" auf „*setup*" gestellt werden. Hierdurch wird ein Domänenbeitritt angestoßen. Damit der Rechner über opsi verwaltet werden kann, muss – wie im vorigen Unterkapitel beschrieben – der *opsi-client-agent* auf dem Rechner vorher installiert sein.

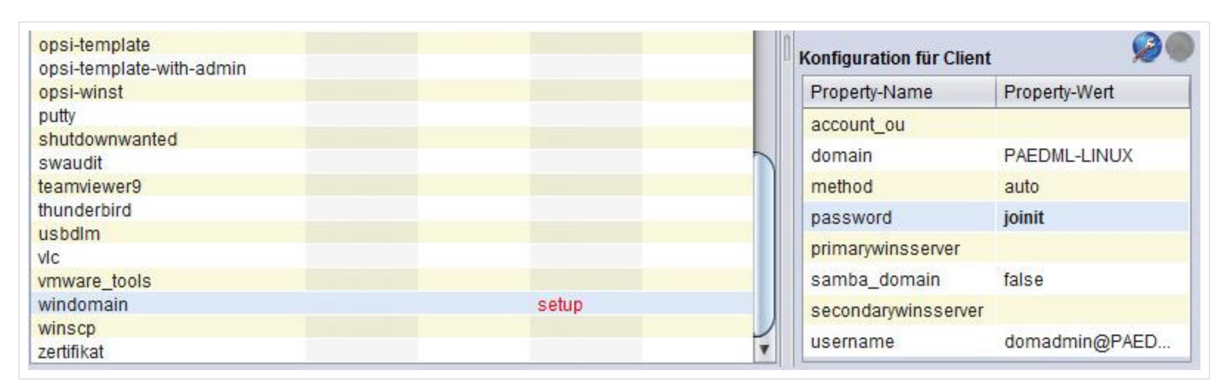


Abb. 171: Domänenbeitritt mittels opsi-Paket „windomain"



Nachdem die hier beschriebenen Schritte ausgeführt worden sind, können Sie den/ die Rechner in der *opsi*-Konsole aufrufen und mit Software versorgen (vgl. Kapitel 7, ab Seite 116).

9. Arbeiten mit lokalen Images von Rechnern



Bitte beachten Sie unbedingt die Hinweise zur Nomenklatur der *paedML Linux* im Anhang A, Seite 295.

opsi ermöglicht Ihnen, lokale Images auf jedem Rechner zu speichern. Dadurch können Sie den Zustand jedes mit *opsi* verwalteten Rechners konservieren und bei Bedarf ohne nennenswerten Aufwand wiederherstellen.

Die Wiederherstellung kann später auch – sofern das System entsprechend konfiguriert ist – durch einen Lehrer im Computerraummodul vorgenommen werden. Dieser Mechanismus kann genutzt werden, um ein defektes Image während des Unterrichts zu reparieren.

Die Funktionen des Erstellens und Wiederherstellens eines Abbildes finden Sie in den „*opsi-local-image*“-Produkten. Im Zusammenhang mit lokalen Images sind die folgenden Netboot-Produkte relevant

3. *opsi-local-image-prepare* – Dieses Modul hilft bei der Einrichtung der Festplatte bei der Erstinstallation.
4. *opsi-local-image-backup* – Hierüber wird ein Image erstellt.
5. *opsi-local-image-restore* – Mit diesem Modul kann ein Image wiederhergestellt werden.
6. *opsi-local-image-delimage* – Mit diesem Modul können alte Images gelöscht werden.

Produkt-ID	Stand	Report	Angefordert	Version
hwinvent				
opsi-local-image-backup				
opsi-local-image-delimage				
opsi-local-image-prepare				
opsi-local-image-restore				
opsi-local-image-win7-x64				
opsi-local-image-win81-x64				
opsi-local-image-win8-x64				
opsi-local-image-winxp				
wipedisk				

Abb. 172: opsi-Produkte im Reiter „Netboot-Produkte“

Durch das Vorhalten lokaler Images ist eine schnelle Restauration von Rechnern möglich, ohne dass Daten über das Netzwerk verteilt werden müssen. Durch die Verteilung von Images wird in der Regel die Netzwerkperformanz in Mitleidenschaft gezogen, da große Datenmengen vom Server auf die Clients und zurück übertragen werden.

Das Vorhalten lokaler Images bietet die Möglichkeit, wertvolle Systemzustände, (z.B. *Windows*-Aktivierungen) zu erhalten, wenn die Images zurückgespielt werden.

9.1 opsi-local-image-prepare

Die Grundvoraussetzung für das Funktionieren der *„opsi-local-image*“-Produkte ist, dass der Rechner mit dem *„Netboot-Produkt*“ *„opsi-local-Image-prepare*“ installiert wurde. Mit diesem *opsi*-Werkzeug wird eine Festplatte so eingerichtet, dass die Festplatte in verschiedene Bereiche partitioniert und eine Backup-Partition angelegt wird (vgl. Kapitel 7.5 auf Seite 134).

9.2 opsi-local-image-backup

Das Anlegen eines Images der Systempartition wird über dieses Modul bewerkstelligt. Ein Abbild wird in der Backuppartition abgelegt. Bei der Imageerstellung werden die folgenden Daten an- und in der Backuppartition des Rechners abgelegt:

- *master.log* – Wann wurde welches Netboot-Produkt mit welchen Optionen ausgeführt?
- *Name-des-Images* – Verzeichnis, das wie das erstellte Image heißt und dieses enthält
- *Name-des-Images/img.ini* – Informationen zum Image
- *Name-des-Images/Name-des-Images* – das Image
- *Name-des-Images/productOnClients.json* – Informationen darüber, welche opsi-Produkte auf dem Client installiert wurden (inkl. Version, Datum usw.)

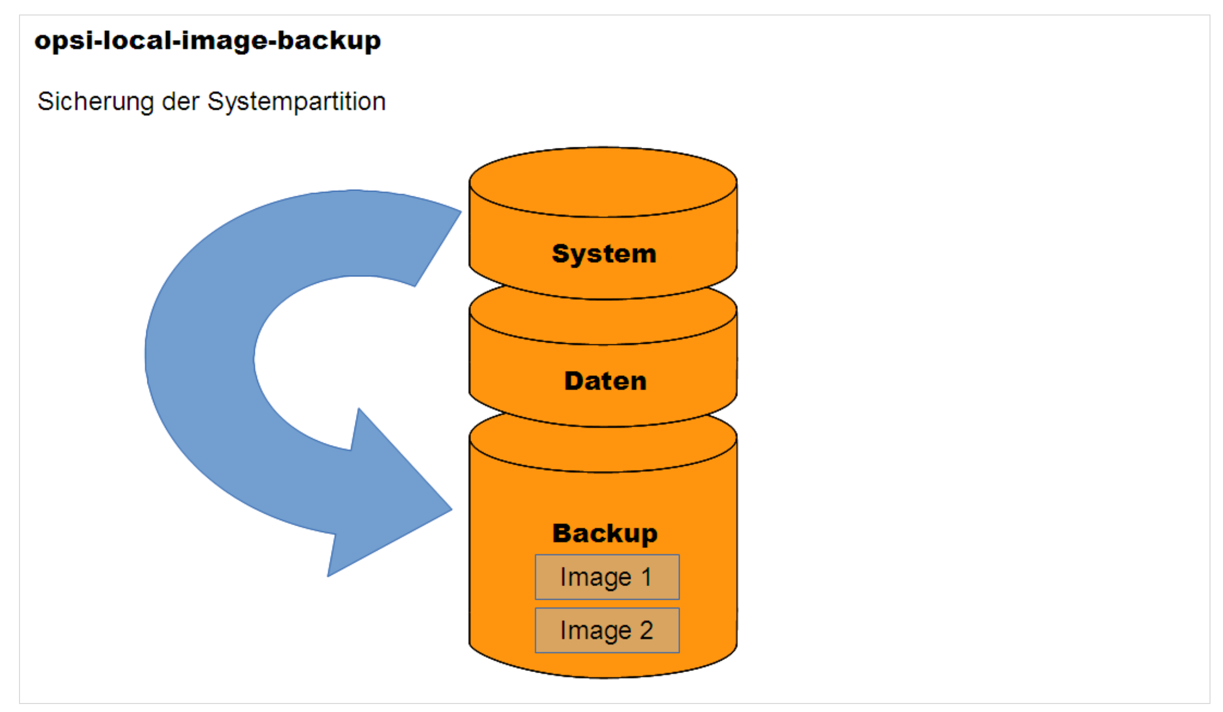


Abb. 173: Sicherung der Systempartition

Die folgenden Einstellungen können Sie für das *Netbootprodukt „opsi-local-image-backup*“ vornehmen:

Property-Name	Property-Wert
askbeforinst	Der Default-Wert (empfohlen) steht auf *„false*“. Wenn Sie die Wiederherstellung durch eine Benutzereingabe bestätigen wollen, Ändern Sie

	den Wert auf „*true*“.
imagefile	Hier kann ein Name eingegeben werden.

Tabelle 20: Werte von opsi-local-image-restore

Beim Ausführen des Backups können Sie einen Namen für das zu erstellende Image eingeben. Sofern manuell kein Name vergeben wird, setzt das System den Namen des installierten „*Netboot-Produktes*“ als Imagenamen, zum Beispiel „*opsi-local-image-win7-x64*“.

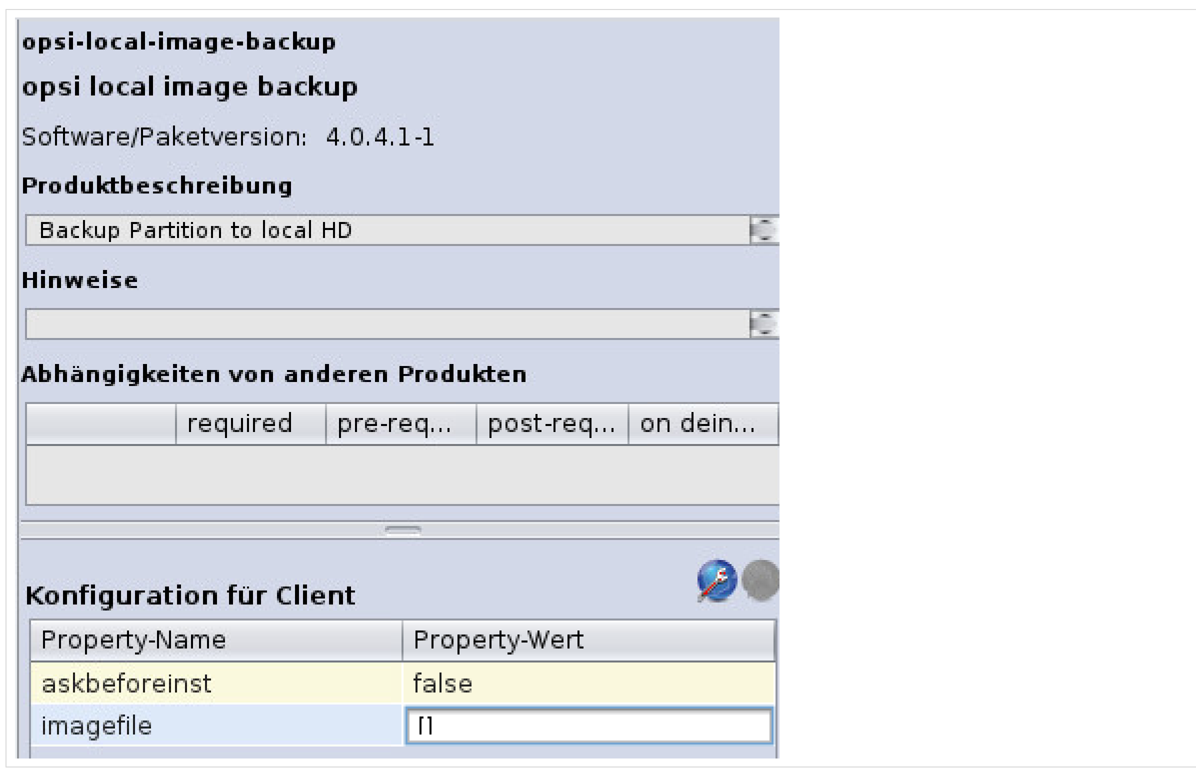


Abb. 174: Einstellungen für „opsi-local-image-backup“

Um einen Namen einzugeben, klicken Sie auf den „*Property Wert*“ von „*imagefile*“. In dem großen weißen Feld sehen Sie – sofern schon Abbilder der Systempartition erstellt wurden – die Namen der alten Images. Unten rechts können Sie den Namen des zu erstellenden Images eingeben. Drücken Sie auf das *PLUS*, um den Namen zu übernehmen. Er erscheint anschließend in dem großen weißen Feld. Sie müssen die Änderungen mit dem Haken übernehmen. Wenn Sie abbrechen wollen, drücken Sie auf den blauen Kreis.



Leerzeichen in opsi-Images werden durch den Unterstrich (_) ersetzt. Sollten Sie ein Image mit Leerzeichen angelegt haben, müssen Sie beim Wiederherstellen das Leerzeichen durch den Unterstrich ersetzen. **Besser ist es, auf Leerzeichen im Imagenamen zu verzichten!**

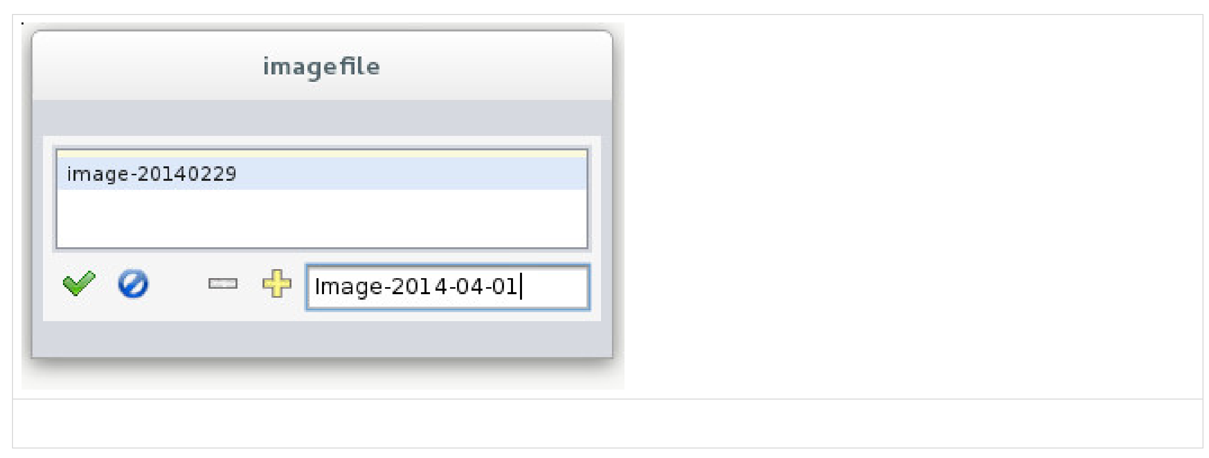


Abb. 175: Eintrag eines Imagenamens

Bitte dokumentieren Sie die Namen der erstellten Images, damit Sie später – wenn Sie mehrere Images haben – wieder darauf zugreifen können. Im Anhang ist eine Tabelle beigefügt, die Sie für die Dokumentation Ihrer Images nutzen können.



Bitte beachten Sie, dass der Imagename „case sensitive“ ist, d.h. dass zwischen Groß- und Kleinbuchstaben streng unterschieden wird und der Imagename später **genau** eingegeben werden muss.

Änderungen in der Konfiguration sind mit dem roten Haken (2) zu bestätigen.



Abb. 176: Geänderte Konfiguration bestätigen

Beim nächsten Systemstart wird das Image erstellt und in der Backup->Prtition gespeichert.



Wenn beim Erstellen eines Images kein Platz mehr in der Backup-Partition vorhanden ist, dann bleibt die Imageerstellung mit der Fehlermeldung „*no space left on device*“ stehen.

In diesem Fall müssten Sie mit *opsi-local-image-delimage* alte Abbilder löschen.

9.3 opsi-local-image-restore

Die Wiederherstellung eines Images wird mit dem Modul *opsi-local-image-restore* ausgeführt. Alle Abbilder, die zuvor in der Backup-Partition eines Rechners abgelegt wurden, können hiermit zurückgespielt werden. Sie können mehrere Images vorhalten und bei Bedarf wiederherstellen.

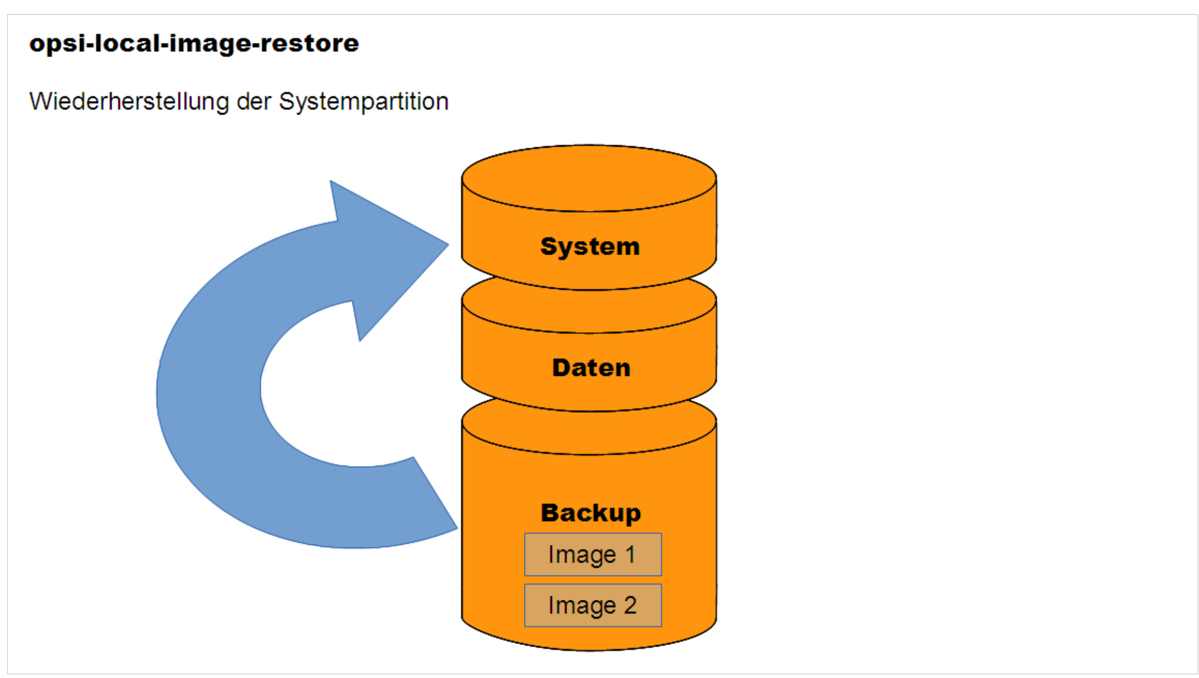


Abb. 177: Wiederherstellung der Systempartition

Die folgenden Einstellungen können Sie für das *Netbootprodukt „opsi-local-image-restore*“ vornehmen:

Property-Name	Property-Wert
askbeforinst	Der Default-Wert (empfohlen) steht auf „*false*“. Wenn Sie die Wiederherstellung durch eine Benutzereingabe bestätigen wollen, ändern Sie den Wert auf „*true*“.
imagefile	Dieser Wert bestimmt, welches Image wiederhergestellt werden soll. Hier ist immer der Wert des letzten Images eingetragen. Wenn Sie ein anderes Image wiederherstellen wollen, müssen Sie den **genauen** Imagenamen aus dem Feld „*imagefiles_list*“ in dieses Feld eintragen.
imagefiles_list	Hier sehen Sie eine Liste aller vorhandenen Images.
method	Dieser Wert definiert, wie das Image wiederhergestellt wird. „*rsync-partclone-image*“ überprüft die Systempartition auf Differenzen zum Image der Backup-Partition und behebt diese („schnelle Wiederherstellung“).

	„*partclone-image-restore*“ stellt das gesamte Image wieder her (länger dauernde vollständige Wiederherstellung).
setup_after_restore	Hier wird festgelegt, welche Produkte nach der Wiederherstellung konfiguriert werden sollen. Default-Eintrag ist „*windomain*“[42].
update_and_backup	Default-Eintrag ist „*false*“. Wenn Sie den Wert auf „*true*“ stellen, überprüft *opsi* nach dem Wiederherstellen eines Images, ob es Software-aktualisierungen für installierte opsi-Produkte gibt, aktualisiert diese und erstellt im Anschluss ein neues Abbild.

Tabelle 21: Werte von opsi-local-image-restore

Konfiguration für Client

Property-Name	Property-Wert
askbeforeinst	False
imagefile	**image-20140229**
imagefiles_list	**image-20140229, image-20140401**
method	rsync-partclone-image
setup_after_restore	windomain
update_and_backup	False

Abb. 178: Einstellungen von opsi-local-image-restore

Änderungen sind mit dem roten Haken zu bestätigen.



Abb. 179: Geänderte Konfiguration bestätigen

Beim nächsten Systemstart wird das Image wiederhergestellt.

9.4 opsi-local-image-delimage

Mit diesem Modul können alte Images aus der Backup-Partition gelöscht werden. Der Wert im Feld „*imagefile*“ ist nicht belegt. Dies bedeutet, dass Sie den Namen des Images wissen müssen, um das Image löschen zu können. Sie können Sich im Modul „*opsi-local-image-restore*“ die Imagenamen im

[42] Hierüber wird der Client erneut in die Domäne aufgenommen. Dies ist notwendig, da das Computerkontopasswort zwischen Client und Domäne regelmäßig neu verhandelt wird und der Computer das aktuelle Kennwort der Domäne unter Umständen nicht im Image hat.

Feld „*imagefiles_list*“ anzeigen lassen und dort abschreiben. Ein Doppelklick auf dieses Feld zeigt eine Liste aller Imagenamen.

Um ein Image zu löschen, tragen Sie den Namen des Images in das Feld „*imagefile*“ ein.

Führen Sie hierfür einen Doppelklick auf das Feld aus. Anschließend können Sie den Namen des zu löschenden Images eintragen und mit dem gelben *PLUS-Symbol* übernehmen. Anschließend im Dialogfenster „*imagefile*“ den roten Haken (der Haken ist zunächst grün und wird nach dem Eintragen des Imagenamens rot) zur Bestätigung drücken.

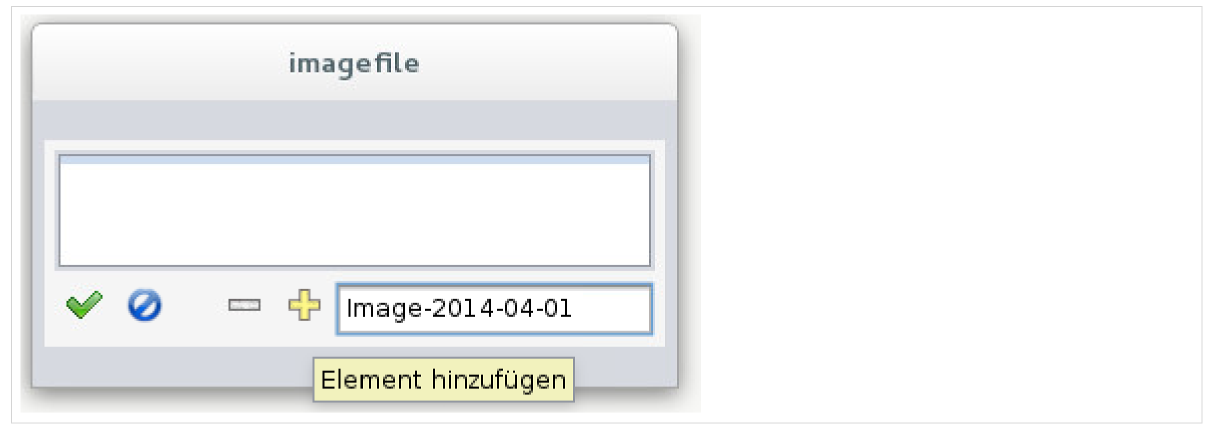


Abb. 180: Löschen eines Images aus dem Cache

Änderungen in der Konfiguration sind mit dem roten Haken (2) zu bestätigen.



Abb. 181: Geänderte Konfiguration bestätigen

Beim nächsten Systemstart wird das Image aus der Backup-Partition gelöscht.

10. Capture-Images



Bitte beachten Sie unbedingt die Hinweise zur Nomenklatur der *paedML Linux* im Anhang A, Seite 295.



1. Aus lizenzrechtlichen Gründen dürfen wir keine Installationsdateien ausliefern. Bitte beachten Sie, dass Capture-Images wie in Kapitel 7.4 „Vervollständigen der opsi-Pakete für die Windows-Installation“ beschrieben, ebenfalls mit Windows-Installationsdateien versorgt werden müssen.
2. Auch das unter Kapitel 7.7 „Treiberintegration“ beschriebene Verfahren zur Integration von Treibern muss für *opsi-capture-Produkte* gesondert angewendet werden.

In den Vorgängerversionen der *paedML Linux 6.0* wurden Clients mit Software versorgt, in dem ein vorher erstelltes Image an die Rechner ausgespielt wurde. Hierfür wurde ein "Muster-Client" erst mit dem Betriebssystem, dann mit zusätzlicher Software (inklusive Treibern installiert. Von diesem Muster-Client wurde ein Abbild (Image) erstellt, das anschließend (über *Linbo* oder *Rembo*) an andere Rechner im Netzwerk verteilt wurde.

Das neue Software-Verteilungsverfahren mit opsi bietet etliche Vorteile. So können Rechner granular mit Software versorgt werden und der Lehrer-PC kann beispielsweise eine andere Software-Ausstattung als die Schüler-PCs eines Raumes erhalten. Dies geschieht ohne, dass Sie mehrere Images vorhalten müssen, zentral über die *opsi-Konsole*.

Für jedes *Windows*-Betriebssystem gibt es ein *opsi-Netboot-Produkt*, in dem die Installations-Dateien abgelegt werden. Installationsdateien werden als *.wim-Datei* – im *Windows-Imaging-Format*[43] – auf dem *opsi*-Server abgelegt.

opsi bietet Ihnen die Möglichkeit über eine neue *.wim-Datei* Änderungen an einer Standard-Installation zu speichern (empfohlen). Hierbei werden nur die Differenzen zum bestehenden Image gespeichert. Die Images bleiben in der Summe schlank, da nicht jedes Mal ein neues komplett Image erstellt wird, wie es etwa bei *Linbo* der Fall war.

Es ist aber auch möglich eine komplett neue .wim-Datei anzulegen, die die Standard-*Windows*-Installationsdatei überschreibt[44].

Wofür wird das Capture-Image benötigt?
In der Regel ist die Installation von Rechnern über die *opsi*-Konsole ausreichend, um alle Rechner im Schulnetz zu installieren. Es gibt durchaus Situationen, in denen die Softwareverteilung von opsi an ihre Grenzen kommt:

---

[43] http://de.wikipedia.org/wiki/Windows_Imaging_Format_Archive

[44] Der Parameter „*capture_mode*“ bestimmt das Verhalten des Capture-Prozesses. „*append*“ (s.u.) hängt neue Daten an das bestehende Image an, „*always_create*“ erstellt ein neues Image.

- Die Installation von Treibern mit *opsi* setzt das Vorhanden-Sein einer *.inf-Datei* voraus. Leider gibt es Hardware, die mit Treibern ausgeliefert wird, die nur als ausführbare Datei (.exe) vorliegt. Diese Treiber müssen manuell auf den Clients installiert werden.
- Software, die installiert werden soll, liegt nicht als *opsi*-Paket vor.

Hier kommt das *opsi-Capture-Image* ins Spiel, mit dessen Hilfe Sie von einem über *opsi* installierten Rechner ein Abbild, in Form eines angepassten *Windows*-Setups (*.wim-Datei*), erstellen und an andere Rechner im Netzwerk verteilen können.



1. Damit Sie mit *opsi-Capture-Image* ein Abbild erstellen und verteilen können, müssen die beteiligten Rechner mit *opsi* (*opsi-local-image-prepare*) installiert worden sein. Nur, wenn die *opsi*-Partitionierung vorliegt, kann mit OPSI ein Capture-Image erstellt werden.

2. Die Rechner, von denen ein Abbild erstellt wird, werden mit *Sysprep* [45] entpersonalisiert. Hierbei werden alle Rechner-spezifischen Informationen gelöscht. Diese Geräte sollten automatisch lokal gesichert werden und nach dem Erstellen des Capture-Images sollten die Geräte aus dem lokalen Cache wieder hergestellt werden.

3. Ein Rechner, auf den das Image ausgespielt wird, muss im Anschluss ggf. erneut aktiviert werden, da es sich um eine quasi-Neuinstallation handelt.



Das hier beschriebene Verfahren hat den Vorteil, dass ein Hardware-unabhängiges Image erstellt wird. Installierte Treiber werden von *Sysprep* entfernt. Wenn das Image auf eine andere Hardware installiert wird, installiert *opsi* - sofern hinterlegt - die hardware-spezifischen Treiber der neuen Hardware und das Image läuft auf einem anderen Gerät[46].

10.1 Ablauf

Eine kurze Übersicht über den Ablauf der Image-Erstellung und –Verteilung:

- Der Muster-Client muss mit *opsi* installiert worden sein.
- Der Muster-Client, von dem ein Abbild erstellt werden soll, muss komplett (Betriebssystem, Software, optionale Treiber) installiert werden.
- Bevor ein *Capture-Image* erstellt wird, überprüft *opsi*, ob es bereits ein lokales Image (*local-image*) gibt. Sofern es kein lokales Image gibt und auch keines erstellt werden soll (Voreinstellung), bricht *opsi* den Vorgang ab.

  Achtung: opsi überprüft hierbei nur, ob es ein Image gibt. Dieses Image muss nicht dem aktuellen Softwarestand des Clients entsprechen!

[45] http://de.wikipedia.org/wiki/Sysprep

[46] Je nach Hardware-Ausstattung müssen ggf. Treiber installiert werden.

- (optional:) Vor der Imageerstellung wird ein neues Image erstellt (empfohlen).
- Im nächsten Schritt wird der Rechner mit Hilfe von *Sysprep* entpersonalisiert. Hierbei werden beispielsweise hardware-spezifische Informationen (u.a. auch Hardwaretreiber) und Lizenzinformationen gelöscht.
- Ein neues, entpersonalisiertes Abbild wird erstellt und die Image-Dateien werden auf den Server geladen.
- Nach der Erstellung des *Capture-Images* wird das letzte funktionierende Image des Muster-Clients wieder hergestellt (Auslieferungszustand).
- Das neu erstellte *Capture-Image* kann auf beliebige Rechner im Netzwerk ausgespielt werden.

10.2Erstellen von Capture-Images



Es wird dringend empfohlen, dass Sie für das Erstellen von Capture-Images die gesonderten Capture-Produkte verwenden. Die Original-*Windows*-Installationen bleiben dadurch unangetastet.

Wenn Sie Capture-Images verwenden, müssen die Zielprodukte – genauso wie „normalen“ *Windows*installation – gemäß Kapitel 7.4 ab Seite 130 mit *Windows*-Installationsdateien versorgt werden.



In der ersten Verkaufsversion fehlen die *opsi-capture-Produkte*. Wenn Sie keine *opsi-capture*-Produkte auf Ihrem System installiert haben, führen Sie unbedingt das Errata-Update (vgl. http://support-netz.de/technische-unterstuetzung/kundenportal/linux/updates-und-patches/errata-1-update.html) auf Ihrem System aus.

Darin ist auch beschrieben, wie Sie mit den folgenden drei Befehlen die *opsi-Produkte* nachinstallieren können:

```
# ucr set --force opsi/product-
download/repository_uib/includeProductIds=opsi-local-image-
win7-capture,opsi-local-image-win7-x64-capture,opsi-local-
image-win8-x64-capture,opsi-local-image-win81-x64-capture

# opsi-product-updater -i -vvv

# ucr unset --force opsi/product-
download/repository_uib/includeProductIds
```

Befolgen Sie unbedingt die Hinweise in der Errata1-Update-Anleitung, bevor Sie die opsi-Capture-Produkte einsetzen können.

10.2.1 Konfiguration von sysprep

Um ein Image vom Muster-Client abzuziehen, öffnen Sie die *opsi-Konsole* (vgl. im Folgenden die Ziffern der Grafik aus Kapitel 7.3, ab Seite123, die sich auf im Anhang findet) und wählen Sie in der Rechnerübersicht (4) den Rechner, dessen Abbild Sie erstellen wollen.

Im Reiter "*Produktkonfiguration*" des Hauptfensters (5) wählen Sie das Produkt "*opsi-local-image-sysprep*" aus und stellen dieses auf *Setup*, damit der Rechner im ersten Schritt der Image-Erstellung entpersonalisiert wird.



Abb. 182: Auswahl von opsi-sysprep

Die folgenden *Produkt-Werte* können im Bereich „*Konfiguration für Client*" gesetzt werden. (Es wird empfohlen hier nichts zu ändern.):

Property-Name	Property-Wert
abort_on_no_backup	Steht dieser Wert auf "*true*", so überprüft *opsi*, ob es ein lokales Image gibt, das benötigt wird, um den Rechner wieder herzustellen nachdem die Installation mit *Sysprep* unbrauchbar gemacht wurde. Existiert kein solches Image, bricht der Vorgang ab. **Dieser Wert MUSS auf „*true*" belassen werden, andernfalls muss der Rechner neu installiert werden.**
always_backup_before_sysprep	Der Wert "*true*" bewirkt, dass ein neues lokales Image erstellt wird, bevor mit *Sysprep* ein neues Abbild erstellt wird. Dieser Wert kann geändert werden.
disabled	Dieses Feld deaktiviert *sysprep*, wenn der Wert „*true*" eingetragen wird. Um *sysprep* auszuführen muss hier also der Default-Wert „*false*" eingetragen sein.
startCapture	Dieser Wert ist der Auslöser für das Ausführen des Netboot-Produktes *opsi-local-image-capture*, über das das Abbild des Rechners erzeugt wird. **Er muss auf „true" belassen werden**.

Tabelle 22: Konfigurationsparameter von opsi-sysprep

10.2.2 Konfiguration des Capture-Images

Die Konfiguration der Image-Erstellung wird über das Netboot-Produkt "*opsi-local-image-capture*" vorgenommen, welches im nächsten Schritt konfiguriert werden muss. Wechseln Sie hierfür im Hauptfenster (5) auf den Reiter „*Netboot-Produkte*".

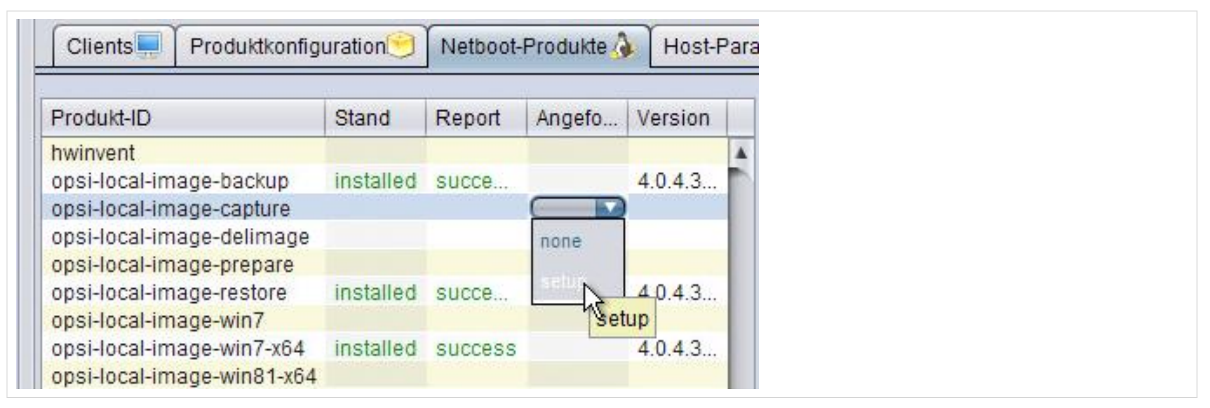


Abb. 183: Auswahl von opsi-local-image-capture

Die folgenden Konfigurationsparameter (Bereich „Konfiguration für Client“) stehen für opsi-local-image-capture zur Verfügung[6]:

Property-Name	**Property-Wert**
askbeforinst	Dieser Wert sollte auf "*false*" belassen werden. Andernfalls muss an der Maschine, von der ein Image erstellt werden soll, der Imaging-Prozess nochmals bestätigt werden.
capture_mode	Belassen Sie die Standard-Einstellung ("*append*"), um die Differenz zu einem bestehenden Image hinzuzufügen. Sie haben die Möglichkeit ein neues Image zu erstellen ("*always_create*"). **Hierdurch wird die Original-Installationsdatei von Windows auf dem opsi-Server überschrieben.**
image_description	Dieses Feld muss befüllt werden. Geben Sie hier eine aussagekräftige Beschreibung ein, um das Image später wieder zu erkennen. (z.B. Standard-Installation_ mit_Lehrer-Tools).
imagename	Geben Sie hier einen aussagekräftigen Namen für das Image ein (z.B. Win7-x64-lehrer). Dieser Name wird später beim Zurückspielen des Images angezeigt.
setup_after_capture	Hier wird ein *Netboot-Produkt* angegeben, dass nach der Imageerstellung ausgeführt wird. Es wird empfohlen den Standard-Wert ("*opsi-local-image-restore*") beizubehalten. Dieser löst ein Restore des Muster-Clients aus, der nach dem Ausführen von *Sysprep* unbrauchbar ist.
target_product	Geben Sie hier an, welchem zugrunde liegenden Betriebssystem das Image zugewiesen werden soll. Der Standardwert ist „opsi-local-image-win7-x64“. Wenn Sie z.B. ein neues Image einer *Windows 8.1* Installation erstellen, dann tragen Sie hier das Netbootprodukt *opsi-local-image-win81-x64* ein. Bei Schreibfehlern wird kein Image erstellt.

Tabelle 23: Konfigurationsparameter für opsi-local-image-capture

Konfiguration für Client

Property-Name	Property-Wert
askbeforeinst	false
capture_mode	append
image_description	**Standard-Installation mit Lehrer-Programmen**
imagename	**capture-lehrer**
setup_after_capture	opsi-local-image-restore
target_product	**opsi-local-image-win81-x64-capture**

Abb. 184: Konfigurationsparameter von opsi-local-image-capture

Sobald Sie den Muster-Client neu starten, laufen die hier beschriebenen Prozesse ab und es wird ein Abbild erstellt, das auf den Server geladen wird. Der folgende Screenshot zeigt den Vorgang des Image-Erstellens. Der Capture-Image-Vorgang dauert einige Zeit, in der nicht an dem Rechner gearbeitet werden kann.

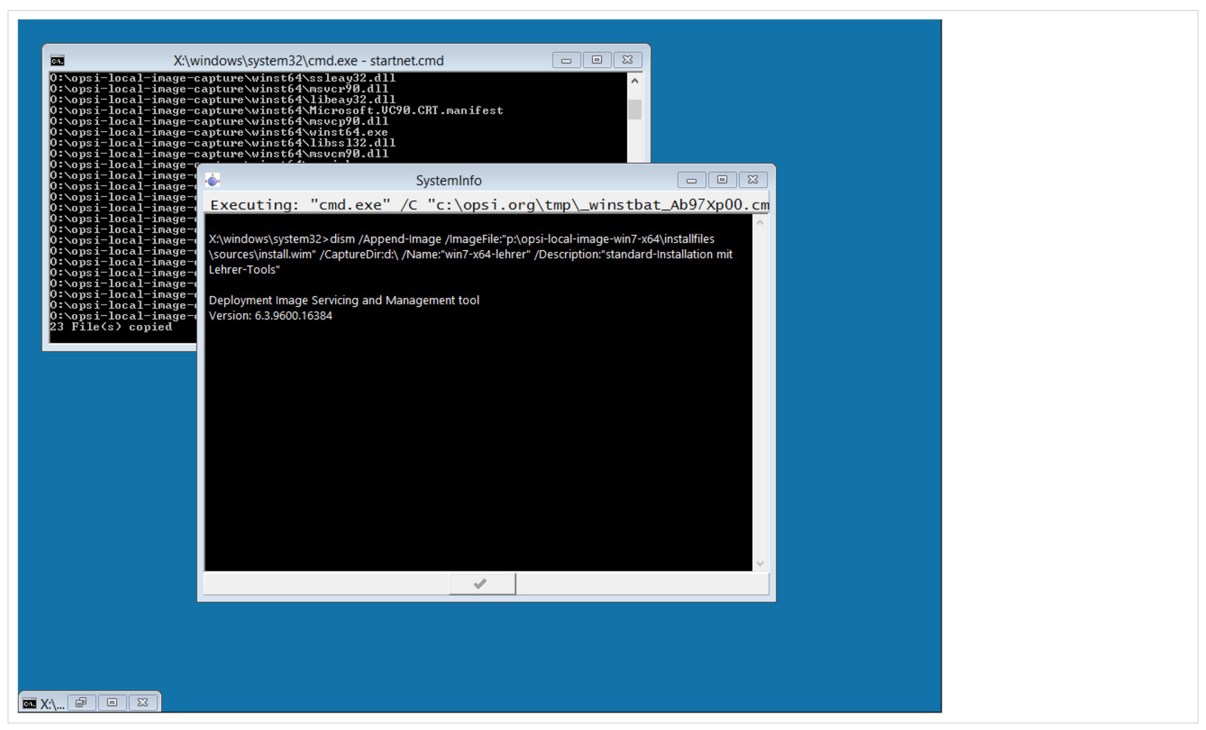


Abb. 185: Erstellen des Abbilds

10.3 Ausspielen eines Capture-Images

Das Ausspielen eines Capture-Images entspricht einer Neuinstallation des Rechners, wobei der Rechner nicht mit dem Standard-Image (bzw. mit einer Standard-*Windows*-Installation), sondern mit einem durch Sie angepassten Capture-Image installiert wird.

Um einen Rechner mit dem neu erstellten Capture-Image zu betanken, wählen Sie den Rechner in der Rechner-Übersicht (4) aus und navigieren Sie im Hauptfenster (5) auf den Reiter "*Netboot-Produkte*".

Stellen Sie das Produkt "*opsi-local-image-prepare*" auf "*setup*". Wählen Sie im Feld „*Konfiguration für Client*“ und dort im „*Property Name*“ „*start_os_installation*“ das *Netboot-Produkt*, das Sie im vorherigen Abschnitt unter „*target_product*“ für das Speichern des Capture-Images gewählt haben.

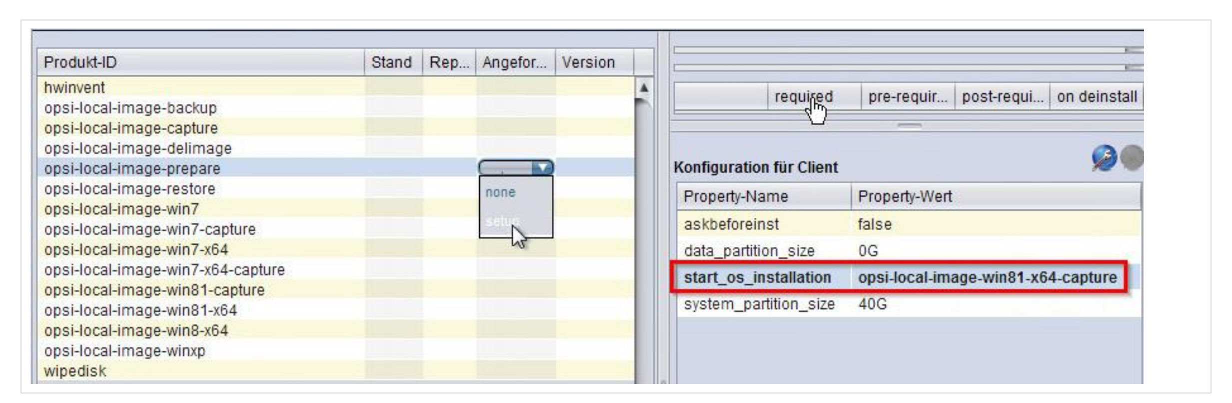


Abb. 186: Auswahl des Netboot-Produktes, das vorher als „target_product“ definiert wurde

Wählen Sie anschließend das „Netboot-Produkt“ („*target-product*“), dem Sie das Capture-Image zugewiesen haben, aus. Im hier beschriebenen Beispiel wurde das Capture-Image „*capture-lehrer*“ dem Netboot-Produkt „*opsi-local-image-win81-x64-capture*“ zugewiesen.

Überprüfen Sie die Werte im Feld „*Konfiguration für Client*“. Der „*Property-Name*“ „*imagename*“ muss nun dergestalt angepasst werden, dass nicht die Standard-*Windows*-Installation (*Windows 8.1*), sondern das Capture-Image installiert wird. In diesem Beispiel das Image mit dem Namen „*capture-lehrer*“.

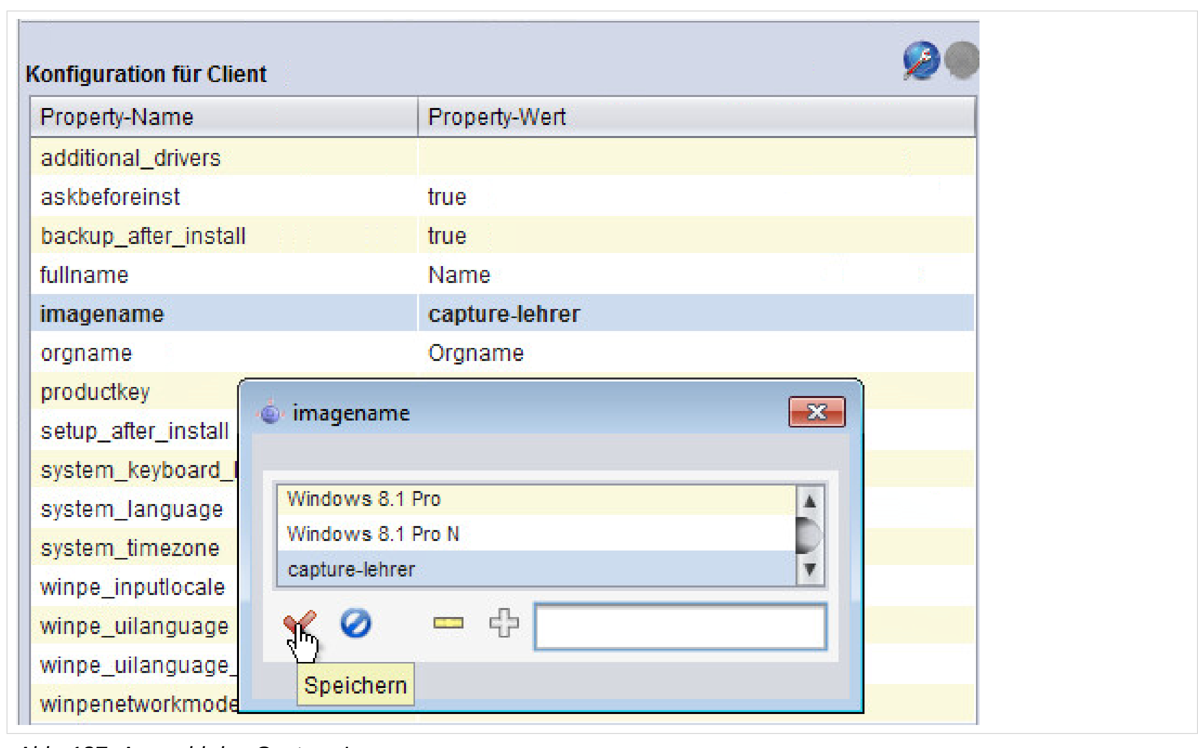


Abb. 187: Auswahl des Capture-Images

Wenn diese Einstellungen getätigt wurden, müssen Sie die Konfiguration abschließend speichern (roter Haken).



Beim nächsten Start des Clients wird dieser mit dem Capture-Image installiert.

11. Gruppenrichtlinien für Windows-Clients



Die Konfiguration von Gruppenrichtlinien ist komplex und benötigt Einarbeitung. Wenn Sie nicht wissen, wie die Konfiguration von Gruppenrichtlinien vorgenommen wird, steht Ihnen die Linux-Hotline mit Rat und Tat bei der Konfiguration der Gruppenrichtlinien zur Seite.

Wir empfehlen dringend, nur dann eigenständig in das System einzugreifen, wenn Sie wissen, was Ihre Änderungen bewirken.

Außerdem ist es ratsam, Änderungen zu dokumentieren, um im Fehlerfall die Suche zu vereinfachen.

Übersicht

- Im ersten Abschnitt dieses Kapitels erhalten Sie grundlegende Informationen zu den Gruppenrichtlinien in der paedML Linux.
- Das darauf folgende Unterkapitel (Kapitel 11.2, ab Seite185) gibt eine Kurzeinführung in die Bearbeitung von Gruppenrichtlinien.

11.1 Gruppenrichtlinien in der paedML Linux

Mit der Einführung von Samba 4 in die *paedML Linux* wurde die Möglichkeit geschaffen „*Windows*-Bordmittel“ in die *paedML Linux* zu integrieren. Durch Gruppenrichtlinien bietet *Windows* eine effektive Möglichkeit die Einstellungen von Rechnern im Netzwerk zu steuern.

Durch Gruppenrichtlinien kann zentral eingestellt werden, wie die Arbeitsplätze der Anwender konfiguriert werden. Hierdurch können Benutzer-Gruppen mit Programmen versorgt oder Drucker an Rechner zugewiesen werden. Sie können Rechte für das Ausführen von Funktionen beschränken oder für bestimmte Benutzer erweitern.

Die *paedML Linux* wird mit vordefinierten *Windows*gruppenrichtlinien ausgeliefert, die bei der Installation von *Windows*-Clients auf den Arbeitsplatzrechnern eingerichtet werden. Man kann dabei zwei Arten von Gruppenrichtlinien unterscheiden:

- Zum Einen sind in der *paedML Linux* Gruppenrichtlinien definiert, die das Verhalten von Rechnerprofilen steuern. Diese Gruppenrichtlinienobjekte tragen den Begriff „*Workstations*“ in Ihrer Bezeichnung.
- Zum Anderen gibt es Gruppenrichtlinien, die das Verhalten von Benutzerprofilen regeln. Die Gruppenrichtlinien tragen den Begriff „*Benutzer*“ im Namen.

Anmerkung: mit Hilfe der Gruppenrichtlinien werden beim Start von *Windows*-Sitzungen Skripte aufgerufen, die ihrerseits Anpassungen an den Einstellungen von *Windows* vornehmen und die Rechner für den Einsatz in der Schule konfigurieren.

Diese Skripte liegen in der Netzwerkfreigabe \\server\netlogon\ScriptsML\. Dort gibt es den Ordner „StartUp“, der Skripte enthält, die beim Hochfahren des Rechners abgearbeitet werden und den Ordner „Login“, dessen Skripte bei der Anmeldung eines Benutzers ausgeführt werden.

11.1.1 Aufruf der Gruppenrichtlinienverwaltung

Für das Bearbeiten von Gruppenrichtlinien wird das Gruppenrichtlinienverwaltungs-Programm (*group policy management console*) von *Microsoft* verwendet. Dieses Programm ist Teil des *opsi-Netboot-Produktes ms-rsat*, das auf Rechnern mit *Windows 7* oder höheren *Windows*-Versionen installiert werden kann. Wenn die *AdminVM* gemäß dem Installationshandbuch installiert wurde, ist „*ms-rsat*“ bereits dort installiert.

Um Änderungen an den Gruppenrichtlinien vorzunehmen; Melden Sie sich als **Administrator der Domäne** an dem Rechner an, an dem das *opsi*-Paket *ms-rsat* installiert wurde.

Sie erreichen das Programm über den „*Windows-Start-Knopf* | *Programme/Dateien durchsuchen*“. Geben Sie dort entweder den Suchbegriff „*Gruppenrichtlinienverwaltung*“ ein oder öffnen Sie das Programm direkt mit dem Befehl `gpmc.msc` , der auch aus einer *Windows*-Eingabeaufforderung gestartet werden kann.

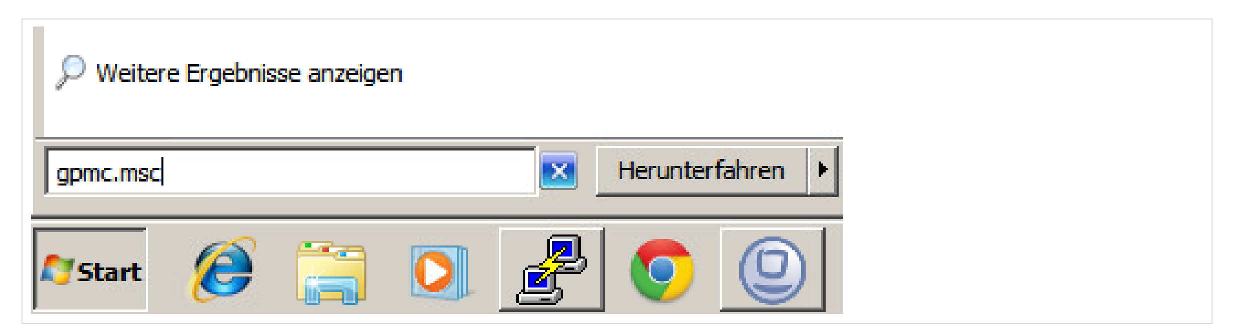


Abb. 188: Ein möglicher Weg den Gruppenrichtlinieneditor aufzurufen

Nach dem Start der Gruppenrichtlinienverwaltung können Sie die Gruppenrichtlinien der *paedML Linux* einsehen.

11.1.2 Aufbau der Gruppenrichtlinienverwaltung

Die Gruppenrichtlinienverwaltung ist ein mächtiges Werkzeug, mit dem verschiedene Domänen, darin befindliche Organisationseinheiten („organisation unit“ = „OU“), einzelne Rechner sowie Benutzer-gruppen und einzelne Benutzer verwaltet werden können. Einige Ebenen des Programmes, die für den Administrator einer großen *Windows*domäne wichtig sind, klammern wir hier aus, da diese Ebenen für die Arbeit mit der *paedML* nicht relevant sind.

Wenn Sie die Gruppenrichtlinienverwaltung öffnen sehen Sie auf der linken Seite eine Baumstruktur, über die verschiedene Ebenen aufgerufen werden können. Relevant für die Arbeit mit der paedML sind folgende zwei Bereiche:

- Im Container „*schule*“ (roter Kasten) finden Sie alle Gruppenrichtlinien, die in Ihrem Schulnetz im Auslieferungszustand bereits aktiviert sind.

- Im Container „*Gruppenrichtlinienobjekte*“(grüner Kasten) finden Sie alle verfügbaren Gruppenrichtlinien (aktive und inaktive). Hier sind unter Umständen Gruppenrichtlinien vorhanden, die nicht im Netzwerk aktiv sind.

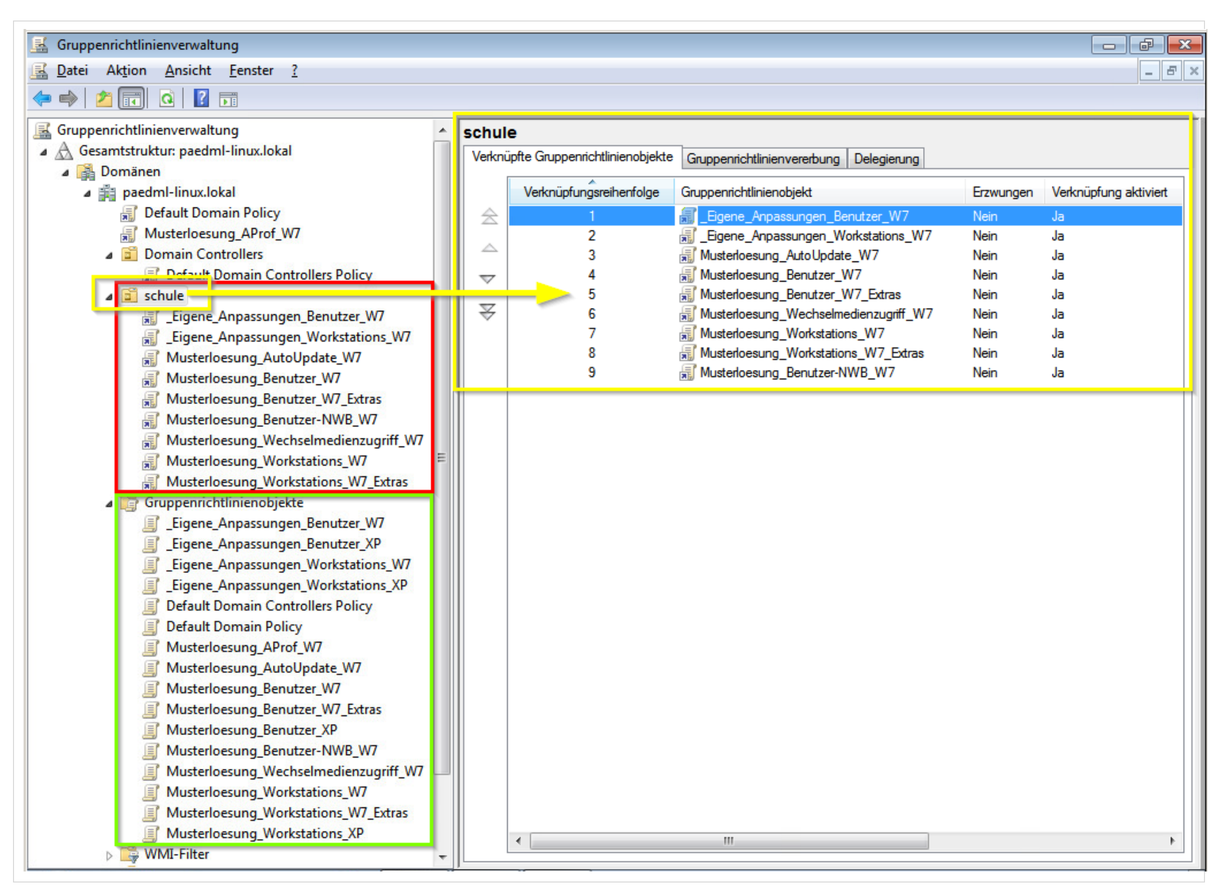


Abb. 189: Der Gruppenrichtlinieneditor und die Gruppenrichtlinien in der paedML Linux

Auf der rechten Seite sehen Sie – sofern der Container „*schule*“ angewählt ist – in welcher Reihenfolge die Gruppenrichtlinien abgearbeitet werden (gelber Kasten). Die Gruppenrichtlinien werden von unten nach oben abgearbeitet. Das heißt die Gruppenrichtlinie mit der kleinsten Nummer wird zuletzt bearbeitet.

Bei „widersprüchlichen“ Gruppenrichtlinien greift daher der letzte ausgeführte Gruppenrichtliniensatz. Diesen Mechanismus nutzen wir im Abschnitt „Änderungen der Gruppenrichtlinien“ (Kapitel 11.2).

11.1.3 Übersicht über die Gruppenrichtlinien der paedML Linux

Die Gruppenrichtlinien lassen sich in verschiedene Kategorien unterschieden, die in diesem Kapitel beschrieben werden.

1. **Rechnerbezogene Gruppenrichtlinien** → „*Musterloesung_Workstations_**“ und „*Musterloesung_AutoUpdate_W7*“
   - Hierin befinden sich Einstellungen, die auf Computer wirken und beim Start der Rechner aktiv werden. Ein Beispiel wäre das Löschen von Profilresten vergangener Sitzungen.
   - Teilweise werden aus diesen Gruppenrichtlinien Skripte aufgerufen, die Änderungen an den Rechnern ausführen.

2. **Benutzerbezogene Gruppenrichtlinien** → „*Musterloesung_Benutzer_**“und „*Musterloesung_Wechselmedienzugriff_W7*“
   - Diese Gruppenrichtlinien wirken beim Anmelden der Benutzer und nehmen Änderungen am Rechner vor, die das Benutzerprofil der Rechner betreffen. Ein Beispiel wäre die Umleitung von Benutzerdaten aus dem lokalen Ordner „Eigene Dateien“ in das Home-Laufwerk auf dem Server.
3. Die Kategorien 1 und 2 lassen sich außerdem nach verschiedenen Betriebssystemen unterscheiden. („*_W7“ – für Rechner ab *Windows* 7 und „*_XP“ für XP-Rechner.
4. Eine Sonderstellung nehmen die Gruppenrichtlinien „*Default Domain Controllers Policy*“ und „*Default Domain Policy*“ ein, die für die Grundfunktionalität des UCS-Domänencontrollers benötigt werden.



Auf der AdminVM werden – sofern das System entsprechend des Installations-Handbuches eingerichtet wurde – keine Gruppenrichtlinien angewandt.

Dadurch werden die Daten der dort arbeitenden Benutzer nicht automatisch nach *H:* synchronisiert und der Administrator hat entsprechend keinen Zugriff auf seine Daten. Außer er sichert diese gezielt auf einer Server-Freigabe.

11.2 Änderung der Gruppenrichtlinien



Nehmen Sie bitte auf gar keinen Fall eigenständig Änderungen an den bestehenden Gruppenrichtlinien „Musterlösung_...“ und „Default_...“ vor!

Es ist notwendig, dass die Hotline bei Problemen im Zusammenhang mit Gruppenrichtlinien auf einen Standard zugreifen kann. Im Bedarfsfall werden die Standardgruppenrichtlinien wiederhergestellt, so dass Änderungen unwiderruflich verloren gehen.

Wenn Sie eigene Gruppenrichtlinien-Einstellungen festlegen wollen, dann verwenden Sie hierfür die Objekte „*_Eigene_Anpassungen_Benutzer*“ oder „*_Eigene _Anpassungen_Workstations*“. Sie können sich selbstverständlich auch eigene Gruppenrichtlinien definieren.

11.2.1 Aktivieren und Deaktivieren von Gruppenrichtlinien

Um eine aktive Gruppenrichtlinie zu deaktivieren, klicken Sie mit der rechten Maustaste auf den Eintrag (im folgenden Beispiel „*Musterloesung_Wechseldatentraeger_W7*“). Ein Klick auf „*Löschen*“ (roter Rahmen) entfernt die Verknüpfung zur eigentlichen Gruppenrichtlinie aus der Liste der aktiven Gruppenrichtlinien des Containers „schule“. Die Gruppenrichtlinie ist dadurch jedoch NICHT im System gelöscht und kann jederzeit wieder zurückgeholt werden.



Beachten Sie unbedingt, dass im Bereich der Gruppenrichtlinienobjekte NIEMALS das Grupperichtlinienobjekt selbst (im folgenden Screenshot rot hinterlegte Fläche), sondern IMMER NUR die Verknüpfung zu einem Gruppenrichtlinienobjekt (im folgenden Screenshot grün hinterlegt) gelöscht werden darf.

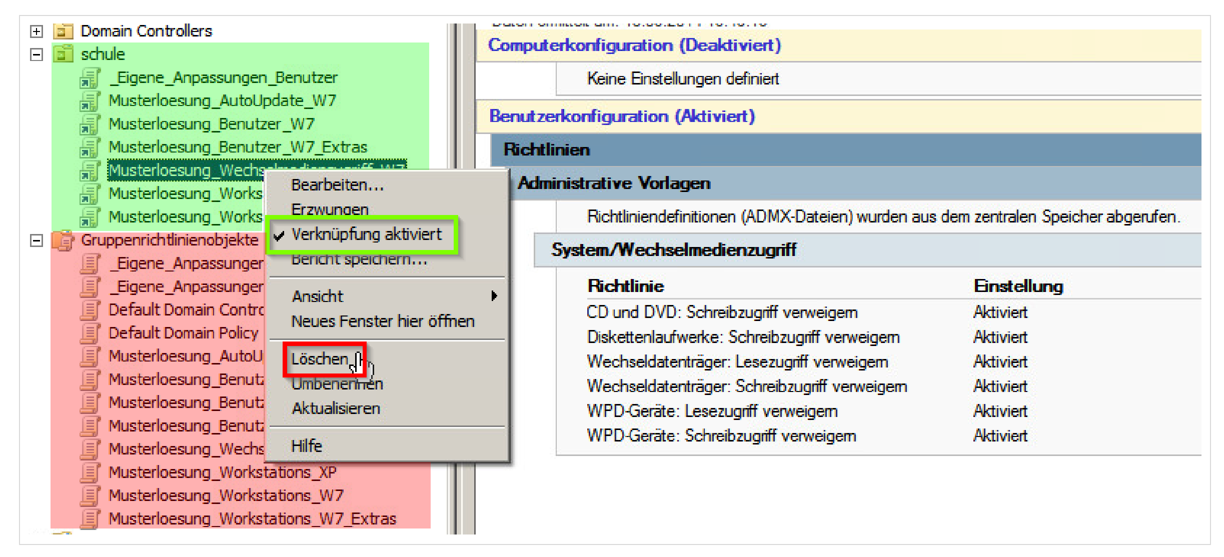


Abb. 190: Deaktivieren einer Gruppenrichtlinie –Achtung! Nicht das Gruppenrichtlinienobjekt selbst löschen!



Ein Haken vor dem Eintrag „*Verknüpfung aktiviert*“ zeigt an, dass die Verknüpfung aktiv ist. Sie können temporär natürlich auch den Haken deaktivieren, wir empfehlen jedoch aus Gründen der Übersichtlichkeit Verknüpfungen auf inaktive Gruppenrichtlinien zu löschen.

Um die gelöschte Verknüpfung zu einer Gruppenrichtlinie wieder herzustellen, klicken Sie mit der rechten Maustaste auf den Container „*schule*“ und wählen dort dein Eintrag „*Vorhandenes Gruppenrichtlinienobjekt verknüpfen*“ aus.

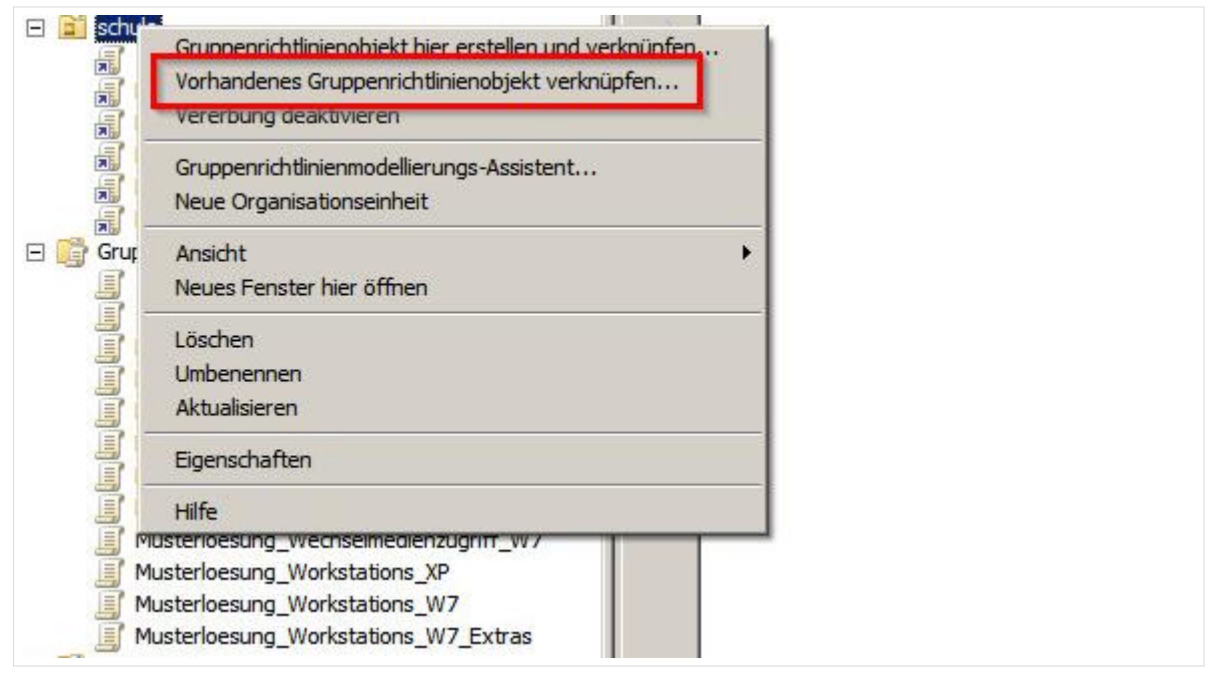


Abb. 191: Gruppenrichtlinienobjekt verknüpfen

Es öffnet sich ein neues Fenster mit dem Titel „*Gruppenrichtlinienobjekt auswählen*“. Wählen Sie das deaktivierte Gruppenrichtlinenobjekt aus und klicken Sie auf „*OK*“. Anschließend wird die Gruppenrichtlinie wieder mit dem Container „*schule*“ verknüpft.

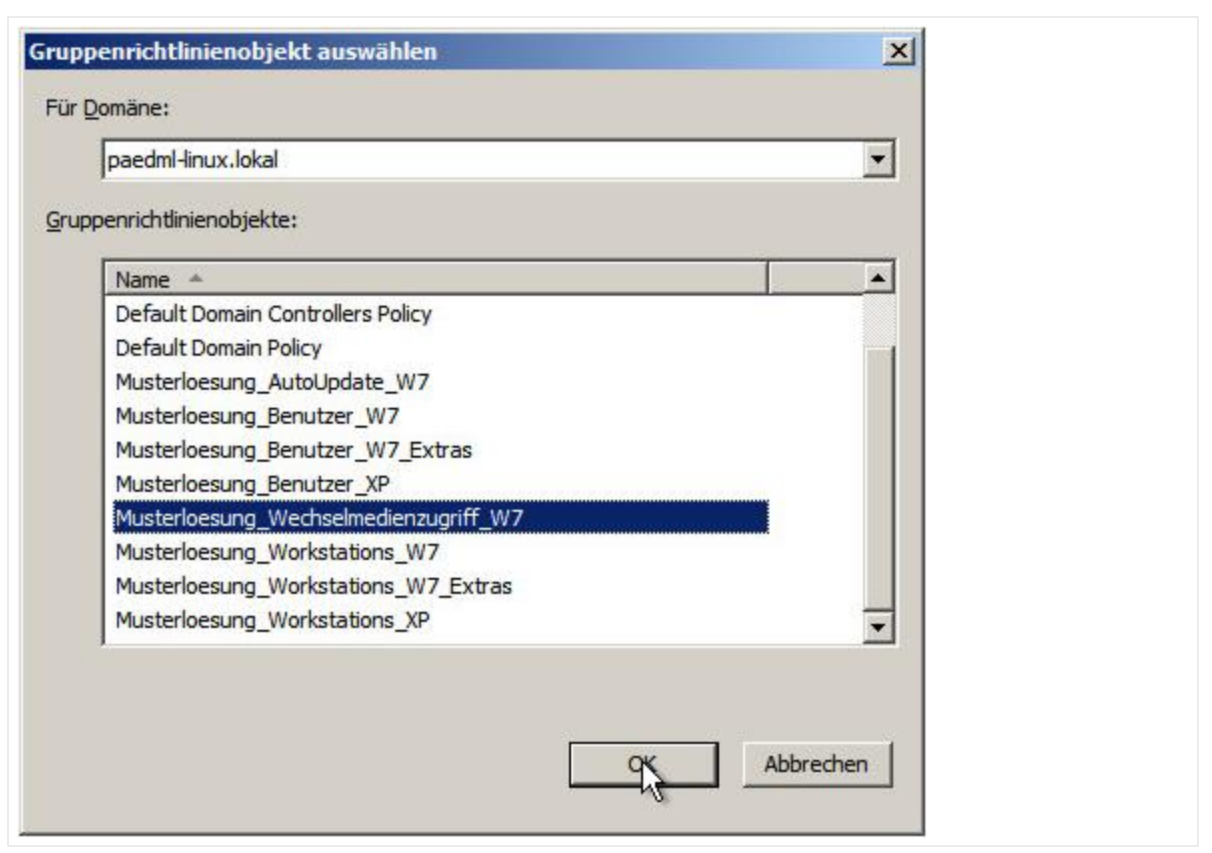
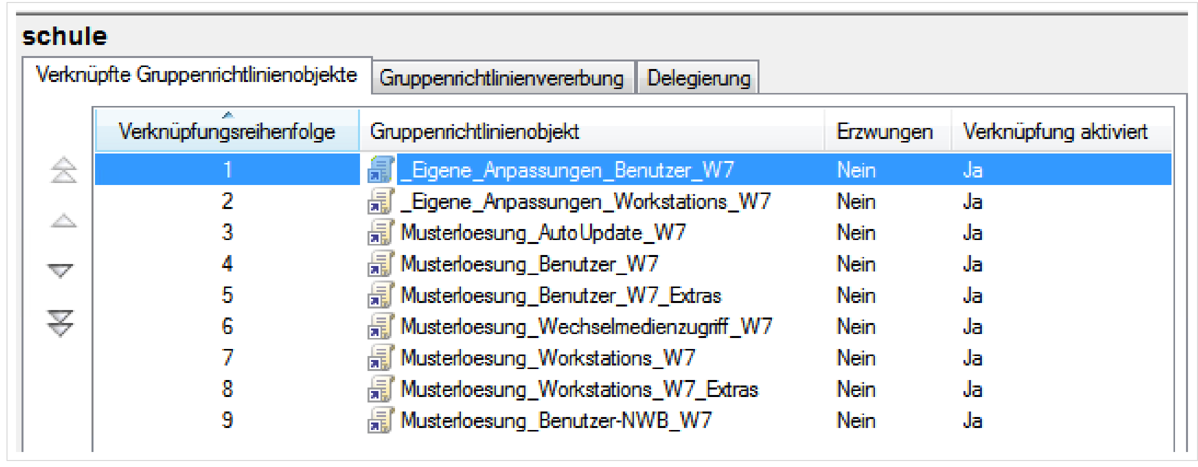


Abb. 192: Auswahl des zu verknüpfenden Gruppenrichtlinienobjektes

Achtung! Die Reihenfolge der Gruppenrichtlinien ändert sich, wenn Sie Gruppenrichtlinien aktivieren und deaktivieren. Sie können die jeweils aktuelle Reihenfolge von Gruppenrichtlinien über die Auswahl des Containers „schule“ in der Gruppenrichtlinienverwaltung aufrufen. Gruppenrichtlinien werden von unten (größere Zahl) nach oben (kleinere Zahl) abgearbeitet.

Uns sind derzeit keine negativen Auswirkungen bei einer geänderten Reihenfolge bekannt, wir empfehlen dennoch die Reihenfolge des folgenden Screenshots einzuhalten:



Verknüpfungsreihenfolge	Gruppenrichtlinienobjekt	Erzwungen	Verknüpfung aktiviert
1	_Eigene_Anpassungen_Benutzer_W7	Nein	Ja
2	_Eigene_Anpassungen_Workstations_W7	Nein	Ja
3	Musterloesung_AutoUpdate_W7	Nein	Ja
4	Musterloesung_Benutzer_W7	Nein	Ja
5	Musterloesung_Benutzer_W7_Extras	Nein	Ja
6	Musterloesung_Wechselmedienzugriff_W7	Nein	Ja
7	Musterloesung_Workstations_W7	Nein	Ja
8	Musterloesung_Workstations_W7_Extras	Nein	Ja
9	Musterloesung_Benutzer-NWB_W7	Nein	Ja

Abb. 193: Reihenfolge der Gruppenrichtlinien in einer Umgebung mit Windows *7 aufwärts.*

11.2.2 Bearbeiten von Gruppenrichtlinien

Die oben aufgestellte Regel, dass Gruppenrichtlinien der *paedML Linux* nicht editiert werden sollen, hat eine Ausnahme, anhand derer die Änderung von Gruppenrichtlinien beschrieben werden kann:

Festlegung der Startseite von Chrome
Die Startseite des Browsers Chrome wird in der Gruppenrichtlinie „*Musterloesung_Benutzer_W7*“ definiert. Wenn Sie statt der Vorgabe www.lmz-bw.de eine eigene Startseite festlegen wollen, dann müssen Sie über die Gruppenrichtlinienverwaltung den Gruppenrichtlinienverwaltungs-Editor öffnen.

Wählen Sie die zu bearbeitende Gruppenrichtlinie mit der rechten Maustaste aus und klicken Sie auf „*Bearbeiten*“.

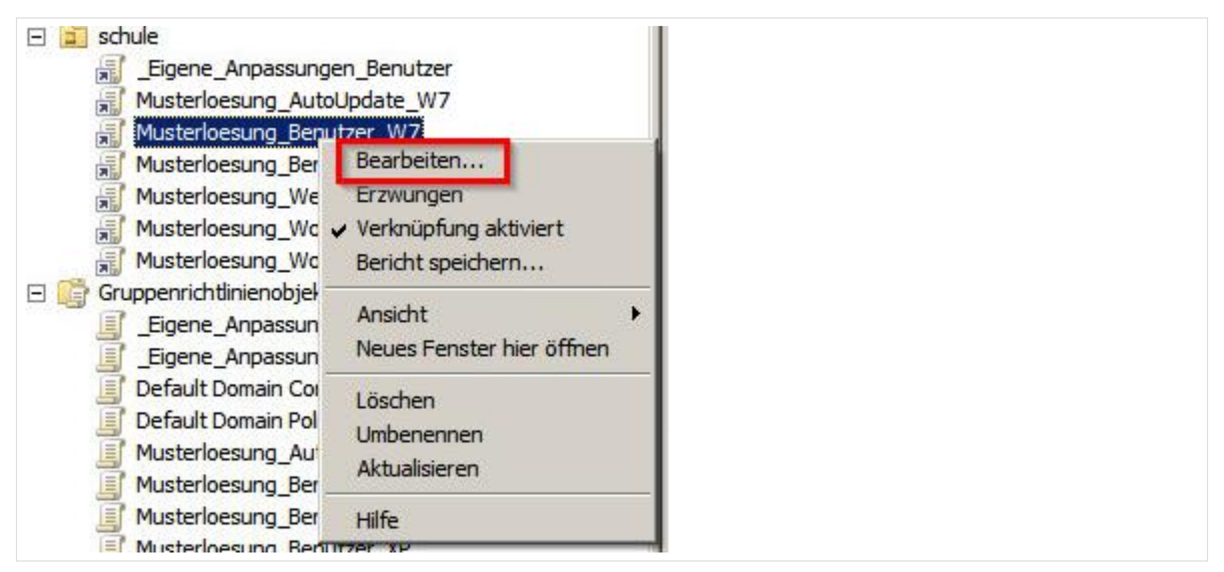


Abb. 194: Aufruf einer zu bearbeitenden Gruppenrichtlinie

Es öffnet sich ein neues Fenster, in dem die Gruppenrichtlinie editiert wird. Sie sehen auf der obersten Ebene der linken Seite den Namen der Gruppenrichtlinie. Die Gruppenrichtlinien der *paedML Linux* sind – wie oben beschrieben – in „*Computerkonfiguration*“ und in „*Benutzerkonfiguration*“ unterteilt. In einer Gruppenrichtlinie könnten theoretisch auch beide Ebenen miteinander konfiguriert werden, die Trennung der Ebenen wurde aber bewusst umgesetzt, um die Konfiguration von Rechner- und Benutzerverhalten zu trennen.

Die konkrete Einstellung verbirgt sich im Zweig „*Benutzerkonfiguration* | *Richtlinien* | *Administrative Vorlagen (…)* | *Google* | *Startseite*“. Der Inhalt des rechten Fenster-Bereichs ist dynamisch und wird je nach Auswahl auf der linken Seite befüllt.

Wenn Sie den Eintrag „*Startseite*“ gewählt haben, dann bekommen Sie auf der linken Seite in den Einstellungen den Eintrag „*Startseiten-URL konfigurieren*“ angezeigt. Ein Doppelklick führt Sie zu einem neuen Fenster, in dem die Startseite des *Chrome*-Browsers geändert werden kann.

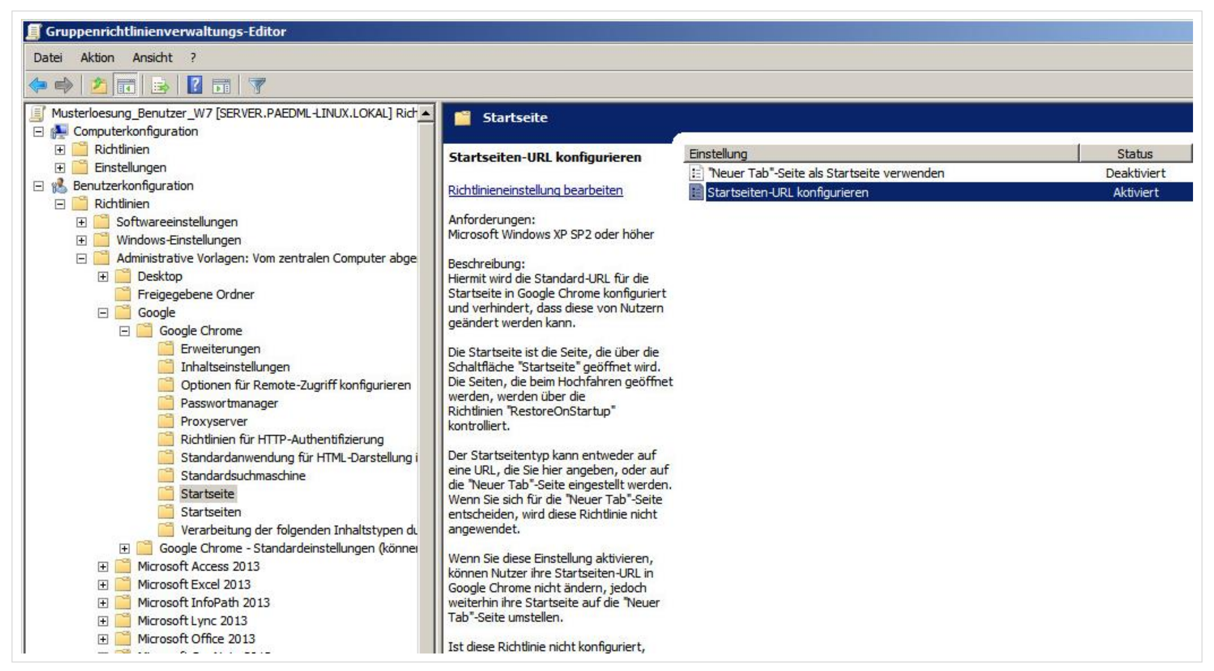


Abb. 195: Der Gruppenrichtlinienverwaltungs-Editor

Die Inhalte, bzw. die Konfigurationsmasken der einzelnen Einstellungen variieren – je nach Parameter, der eingestellt werden soll.

Im vorliegenden Fall wird die Startseiten-URL im Feld „*Optionen*“ definiert. Hier steht im Auslieferungszustand der Wert „*www.lmz-bw.de*“, den Sie anpassen können. Ein Klick auf „*OK*“ speichert die Änderungen.

Damit Änderungen unterhalb der „*Benutzerkonfiguration*“ angewandt werden, müssen die Arbeitsplatzrechner neu gestartet werden. Auch bei Änderungen im Bereich „*Computerkonfiguration*“ müssen die Rechner neu gestartet werden.

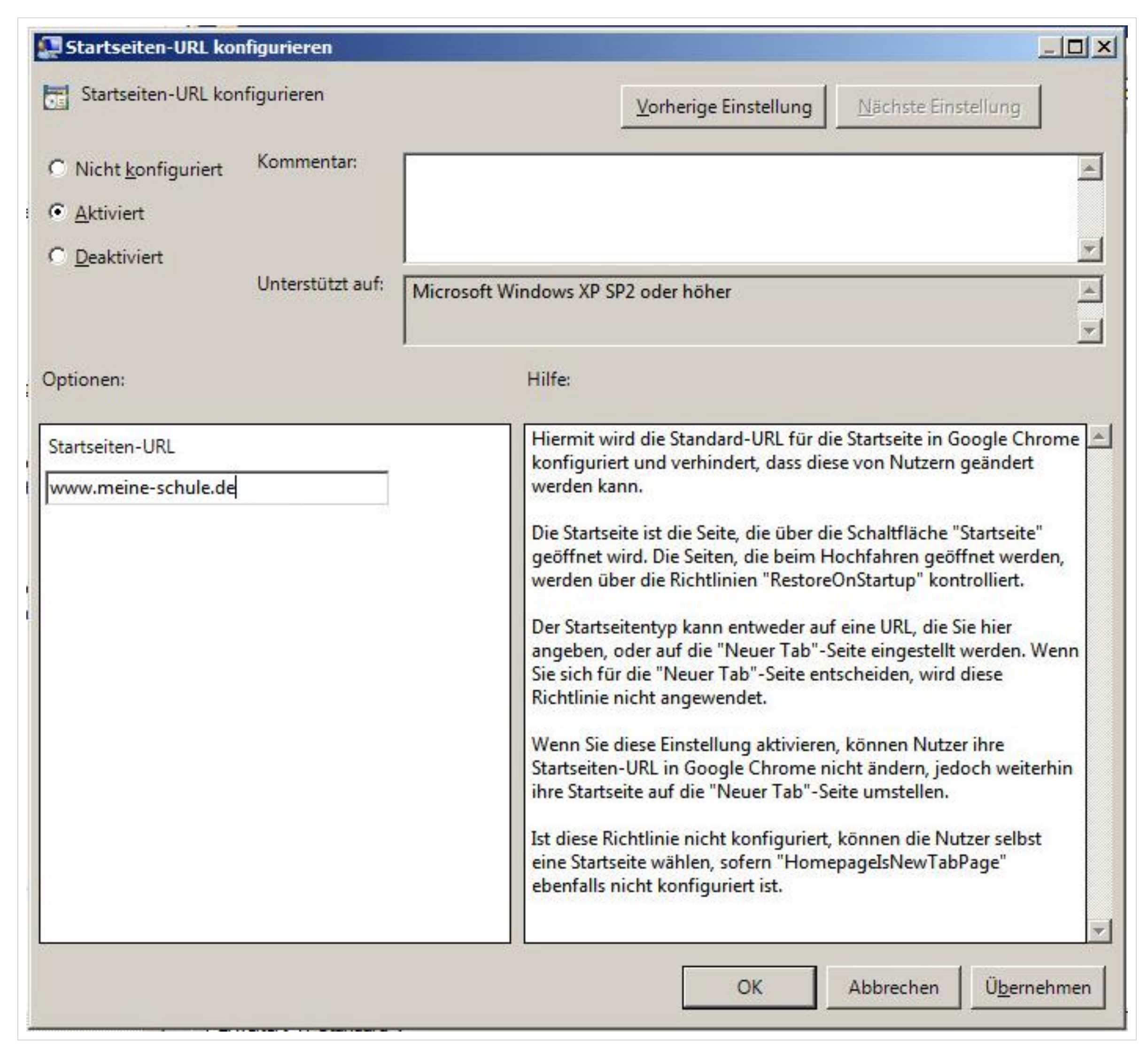


Abb. 196: Änderung der Startseite von google-chrome

12. Weitere Anpassungen der Workstations

In den vorherigen Kapiteln wurden mehrere Wege aufgezeigt, wie Computer in einem *paedML Linux* Netzwerk angepasst werden können. Weitere Anpassungsmöglichkeiten finden Sie in diesem Kapitel.

12.1 Standardprofile für das Kopieren von Desktop-Verknüpfungen

Eine Anforderung bei der Einrichtung von Rechnerprofilen ist die Bereitstellung von Desktop-Verknüpfungen für alle Anwender. Im Unterricht sollten alle Benutzer den gleichen Desktop vorfinden.

Die *paedML Linux* verfügt über zwei Vorlagenbenutzer-Profile, über die Anpassungen an den Desktops der Benutzergruppen vorgenommen werden können:

- Der Vorlagenbenutzer „*AProfLehrer*“ wird für die Einrichtung von Lehrerprofilen benutzt.
- Der Vorlagenbenutzer „*AProfSchueler*“ dient für die Einrichtung von Schülerprofilen.

Die Vorlagen-Benutzer erhalten das Passwort des Benutzers *netzwerkberater*, das bei der Einrichtung von `lmz-initial-setup` vergeben wird.

Die Benutzer-Profile sind nicht zum Arbeiten gedacht - sie dienen nur zum Anlegen von Desktop-Verknüpfungen.

Mit den Benutzerprofilen, die auf dem Server gespeichert werden, können Sie sich an einem Arbeitsplatz der *paedML* Domäne anmelden und Anpassungen vornehmen. Legen Sie Verknüpfungen für ein beliebiges Programme auf den Desktop eines der Vorlagenbenutzer.

Wenn Sie sich abmelden, wird das geänderte Profil auf dem Server gespeichert.

Sobald sich ein Mitglied der Gruppe Lehrer oder Schüler an einem Rechner anmeldet, werden per Gruppenrichtlinie ("*Musterloesung_AProf_W7*") die auf dem Server im Vorlagenprofil gespeicherten Desktopsymbole in das Benutzerprofil des Anwenders geladen.

Zusätzlich kann sich jeder Anwender eigene Verknüpfungen auf dem Desktop ablegen, die nicht überschrieben werden.

Ein Beispiel zur Veranschaulichung:
Auf den Schulrechnern wurde ein Office-Paket installiert. Da die Tabellenkalkulation ein häufig genutztes Werkzeug ist, sollen alle Schüler eine Verknüpfung zum Tabellenkalkulationsprogramm auf dem Desktop erhalten.

Melden Sie sich hierfür als Benutzer „*AProfSchueler*“ an einem Rechner an und erstellen Sie auf dem Desktop die Verknüpfung zu „*Tabellenkalkulation.exe*“ Klicken Sie hierfür mit der rechten Maustaste auf einen freien Bereich auf dem Desktop und wählen Sie „*Neu* **|** *Verknüpfung*“**.** Im ersten Dialogfenster werden Sie nach dem „*Speicherort des Elements*“ gefragt, zu dem Sie eine Verknüpfung erstellen wollen. Wählen Sie hier den Ordner, in dem das Programm installiert ist. Ein Klick auf „*Weiter*“ bringt Sie zum nächsten Dialogfenster, in dem Sie den „*Namen für die Verknüpfung*“ anpassen können. „*Fertig stellen*“ beendet den Dialog.

12.2 Festlegen einer eigenen Startseite von Chrome

In Kapitel 11.2.2 „Bearbeiten von Gruppenrichtlinien“ ab Seite 188 wird beschrieben, wie Sie für Chrome eine eigene Startseite einrichten können.

12.3 Festlegen eines eigenen Hintergrundbildes

Der Desktop-Hintergrund von Rechnern wird über ein Visual-Basic-Skript definiert, das bei jeder Anmeldung ausgeführt wird. Sie finden das Skript mit dem Namen „*SetWallpaper_W7.vbs*“ in der Netzwerkfreigabe *\\server\netlogon\ScriptsML\Login*, die Sie als Domänen-Administrator aufrufen können.

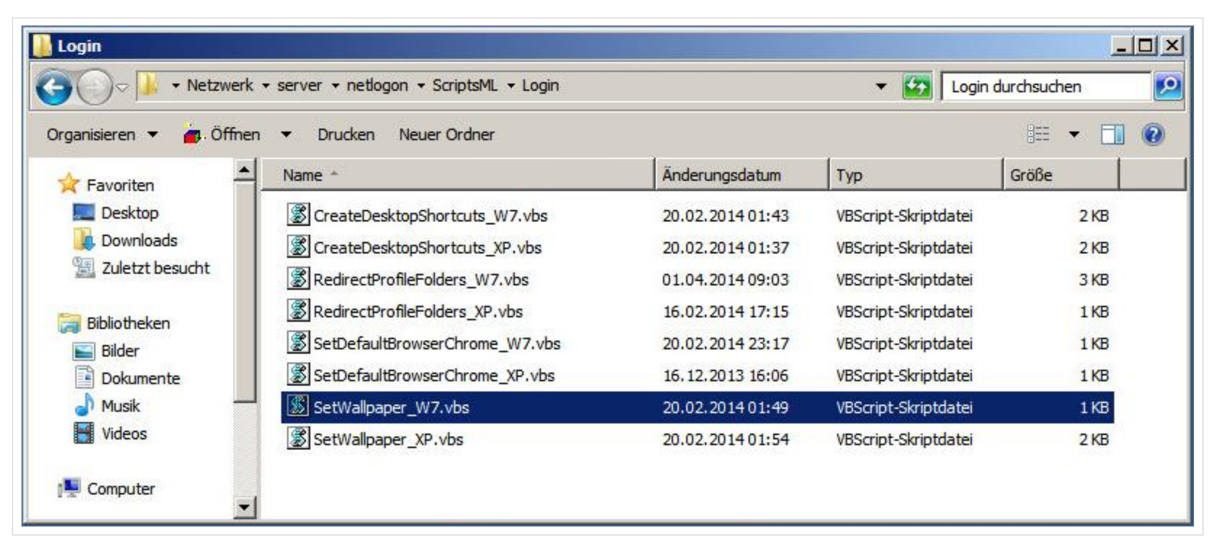


Abb. 197: SetWallpaper_W7.vbs setzt den Desktop-Hintergrund

Mit einem Editor[47] können Sie die Datei aufrufen und bearbeiten. Sie hat den folgenden Inhalt:

```
(…)
Main
Sub Main()
      dim shell
      Set shell = WScript.CreateObject("WScript.Shell")
      'wallpaper = ""
      wallpaper = "\\server\netlogon\hintergrund\beispiel\desktop.jpg"
      'wallpaper = "\\server\netlogon\hintergrund\beispiel\desktop2.jpg"
      shell.RegWrite "HKCU\Control Panel\Desktop\Wallpaper", wallpaper
      shell.Run "%windir%\System32\RUNDLL32.EXE
user32.dll,UpdatePerUserSystemParameters"
End Sub
```

[47] Empfohlen wird *notepad++*.

Mit Hochkomma (‘) startende Zeilen sind auskommentiert und werden beim Skriptaufruf nicht ausgewertet. Wie Sie dem Skript entnehmen können, liegt die Standard-Hintergrunddatei in der Netzwerkfreigabe *\\server\netlogon\hintergrund\beispiel* und heißt „*desktop.jpg*“.

Wenn Sie ein eigenes Hintergrundbild definieren wollen, müssen Sie es in *\\server\netlogon\hintergrund* ablegen und das vbs-Skript ggf. an Ihre Anforderungen anpassen.

12.4 Freigabe von Wechseldatenträgern für Schüler

Wie bereits in der Einführung (Kapitel 1.5, Seite 38) erwähnt, wird durch die Gruppenrichtlinie „*Musterloesung_Wechselmedienzugriff_W7*“ der Zugriff auf externe Speichermedien für Schüler unterbunden. Dies bedeutet im Klartext, dass ein Schüler nicht in der Lage ist auf externe Datenträger (Disketten, CDs, USB-Sticks) oder auf digitale Geräte (Handy, MP3-Player,…), die an den PC angeschlossen werden, zuzugreifen.

Durch diese Einstellungen kann teilweise unterbunden werden, dass durch USB-Sticks oder ähnliches Viren in das Schulnetz gebracht werden – teilweise deshalb, da das Lehrerkollegium natürlich immer noch Schadsoftware einschleppen kann. Auch unerwünschtes File-Sharing kann durch ein Sperren der Datenträger unterbunden werden.

Negativer Seiteneffekt ist jedoch, dass es durchaus Situationen gibt, in dem Schüler Dateien von/auf USB-Sticks ablegen sollen:

- Die Präsentation, die im Unterricht gehalten werden soll kann nicht im pädagogischen Netz abgelegt werden.
- Die Hausarbeit, die in der Schule und zu Hause bearbeitet werden soll kann nach der Fertigstellung nicht ins schulischen Netz gesendet werden.
- Die in der Einführung angesprochene Datensicherung, die zum Ende des Schuljahres verhindern soll, dass die Schüler im neuen Schuljahr aller Daten verlustig gehen, da der Netzwerkberater Tabula Rasa macht und alle Daten aus den Home-Verzeichnissen löscht.

In einem dieser Fälle gilt es natürlich abzuwägen, ob die Sperre von externen Speichermedien (temporär) deaktiviert werden soll.

Das (De-)Aktivieren der Gruppenrichtlinie ist als Beispiel in Kapitel 11.2.1 auf Seite 185 beschrieben.

13. Aktivierung von Windows / MS-Office

Die Aktivierung von *Microsoft*-Produkten ist seit *Windows 7 / Office 2010* notwendig, um die Software betreiben zu können, ohne ständig Systemmeldungen bezüglich nicht aktivierter *Microsoft*-Produkte eingeblendet zu bekommen.

In Vorgängerversionen der *Microsoft*-Produkte war es möglich mit Volumenschlüsseln Software zu installieren und ohne Aktivierung zu betreiben. Seit *Windows 7 / Office 2010* wird die Softwareinstallation an den Rechner, auf dem das Produkt eingesetzt wird, gekoppelt. Pro Rechner wird ein eindeutiger Schlüssel generiert, der über ein Aktivierungsverfahren mit *Microsoft* abgeglichen wird.

Die Aktivierungspflicht hat nichts mit der *paedML* zu tun! Wir unterstützen Sie bei der Aktivierung.

Die Aktivierung eines frisch installierten *Microsoft*-Produktes kann grundsätzlich mit einem der nachstehend genannten Verfahren durchgeführt werden:

- Händisch per Benutzeroberfläche an jedem Client (per Internet oder Telefon, in der Regel sind das Abläufe bei Privatkunden)
- Zentral im LAN über einen *KMS-Server* (Volumenlizenz-Kunden)
- Zentral im LAN über einen *MAK-Proxy* und dem VAMT-Service (Volumenlizenz-Kunden)

Wir empfehlen im Kontext der *paedML Linux* das *MAK-Proxy-Verfahren.* Sie können natürlich auch einen *KMS-Dienst* im Schulnetz betreiben, dieser wird jedoch nicht durch die Hotline unterstützt.



Um *Microsoft*-Produkte – wie hier beschrieben – zu lizensieren benötigen Sie **Volumenlizenzen**. Bitte beachten Sie hierzu die Hinweise in unserem Portal unter

http://www.lmz-bw.de/technische-unterstuetzung/inhalte-pool/info-seite-zu-*Windows*-7-lizenzen.html

Die Hauptvorteile des *MAK-Proxy*-Verfahrens lassen sich wie folgt darstellen:

- Zentrales Auslösen des Aktivierungsvorgangs auf vielen Rechnern mit einem Befehl (Massenaktionen)
- Visualisierung des Aktivierungs-Zustands mehrerer Rechner im Netzwerk "auf einen Blick"
- Re-Aktivierung eines per Selbstheilung wiederhergestellten PCs ohne Belastung des Aktivierungs-Zählers (vgl. Kapitel 13.6, Seite 219)

Beim letztgenannten Vorteil geht es um die "Proxy-Funktion" des *VAMT*-Tools, in diesemZusammenhang also um die Fähigkeit, eine bereits von *Microsoft* erhaltene Aktivierungsbestätigung für eine Arbeitsstation zwischenspeichern und wiederverwenden zu können.

Eine wichtige Grundvoraussetzung für die vorgenannten Massenaktionen ist, dass die Rechner im Schulnetz eingeschaltet und mit dem Netzwerk verbunden sind.

Idealerweise weckt der Netzwerkberater zur Durchführung dieser Arbeiten die Clients in einem ungenutzten EDV-Raum per Wake-On-LAN-Funktionalität auf. Es genügt, die Arbeitsstationen nach dem Aufwecken hierfür im Zustand der "Anmeldemaske" zu belassen.

Sie benötigen für die Aktivierung der *Microsoft-Produkte* mittels *VAMT* die folgenden opsi-Pakete, die auf der *AdminVM* installiert werden sollten[48]:

- *ms-vamt* – Das Volume Activation Management Tool, über das die Aktivierung stattfindet.
- *ms-powershell* – Die *Windows-Powershell* ist eine Weiterentwicklung des Kommandozeilenprogrammes cmd.exe. Die Version 3.0 ist im Standard-Installationsumfang von *Windows 7* enthalten und wird daher nachinstalliert.
- *ms-sql-2012ee* – Der *Microsoft*-SQL-Datenbank-Server, der als kostenlose „Light"-Version vorliegt. Hiermit werden die Aktivierungsinformationen seit *VAMT 3.0* abgespeichert.



Die Aktivierung von *Windows* oder *Microsoft Office* erfordert seit *Windows 8* bzw. *Office 2013* die *VAMT* Version *3.0*

Dieses Programm benötigt einen Datenbankserver. Hierdurch wird die Konfiguration aufwändiger als beim „alten" VAMT-Werkzeug, mit dem Vorgängerversionen der *Microsoft-Produkte* aktiviert wurden.

Wenn Sie NUR *Windows* 7 oder Office 2010 Einsatz haben, können Sie mit einer alten VAMT-Version arbeiten, die auf den Datenbankserver verzichtet. Eine Anleitung zur Einrichtung mit VAMT 2 finden Sie unter:

http://supportnetz.de/fileadmin/user_upload/Technische_Unterstuetzung_SPN/Dateien/6_Kundenportal/4_Lernsoftware__MSI-Pakete_/paedML-*Windows*-Anleitung-Aktivierung-Office2010.pdf

Für die Einrichtung des *Windows*aktivierung sind die folgenden Schritte notwendig:

Als lokaler Administrator:

1. Anlegen eines Datenbankprofils für den Domänen-Administrator
2. Anlegen einer neuen VAMT-Datenbank

Als Domänen-Administrator:

3. Aufruf von VAMT und Einrichtung der Aktivierung (wird durchgeführt als Administrator der Domäne).
4. Aktivierung (wird durchgeführt als Administrator der Domäne).



Das Support-Netz haftet nicht für etwaige Folgen einer fehlerhaften Anwendung der hier beschriebenen *Microsoft*-Aktivierungswerkzeuge.

Eventuell entstehender Kommunikationsbedarf mit der zuständigen *Microsoft*-Hotline („*Microsoft* Product Activation Center"), welcher das Vertragsverhältnis zwischen

---

[48] Bei der Auswahl des opsi-Paketes *ms-vamt* werden die Pakete *ms-powershell* und *ms-sql-2012ee* automatisch selektiert und mit installiert.

dem jeweiligen Lizenznehmer (Schule bzw. Schulträger) und *Microsoft* betrifft, wird nicht von der Support-Netz-Hotline übernommen.

13.1 Datenbankprofil für den Domänen-Administrator anlegen

Das opsi-Paket *ms-sql-2012ee* installiert den *Microsoft SQL Server 2012*. Der Datenbankserver läuft lokal und wird vom lokalen Administratorprofil verwaltet.

Die Verwaltung der Lizenzdaten wiederum geschieht über das Konto des Administrators der *paedML*-Domäne. Dieser Benutzer hat zunächst keine Zugriffsrechte auf lokale Datenbanken. Daher müssen Sie diesen Benutzer im SQL-Server einrichten.

Melden Sie sich hierfür an der *AdminVM* als **lokaler** `Administrator` an. Wenn Sie das Kennwort nicht geändert haben, ist das Standard-Kennwort für die lokale Anmeldung `nt123`.



Abb. 198: lokale Anmeldung an der AdminVM

Unter „*Start* | *Programme* | *Microsoft SQL Server 2012*“ finden Sie die Verknüpfung „*SQL Server Management Studio*“ mit dem der SQL-Server verwaltet wird.

Rufen Sie die Verknüpfung auf und legen Sie sich ggf. eine Kopie der Verknüpfung auf den Desktop, um später schneller darauf zugreifen zu können.

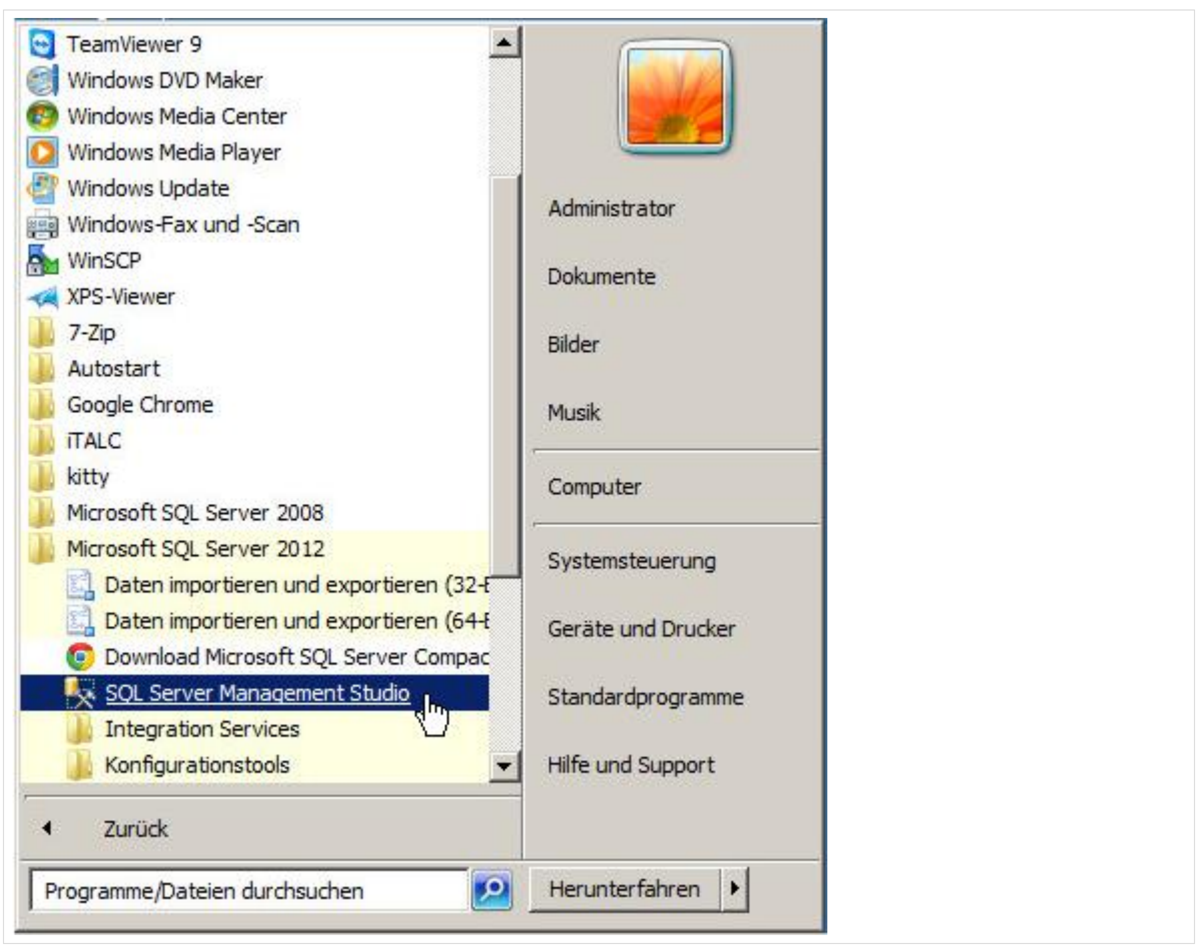


Abb. 199: Aufruf „SQL Server Management Studio“

Das Programm öffnet sich und Sie bekommen einen Dialog „*Verbindung mit dem Server herstellen*“ angezeigt. Überprüfen Sie, ob die Einstellungen richtig sind. Die Datenbank sollte lokal liegen (Feld „*Servername*“ sollte den Namen der Maschine beinhalten). Die Authentifizierung sollte auf „*Windows-Authentifizierung*“ stehen.

Klicken Sie auf „*Verbinden*“, um den SQL-Server aufzurufen. Anschließend wir der „*Objekt-Explorer*“ mit Inhalt gefüllt.

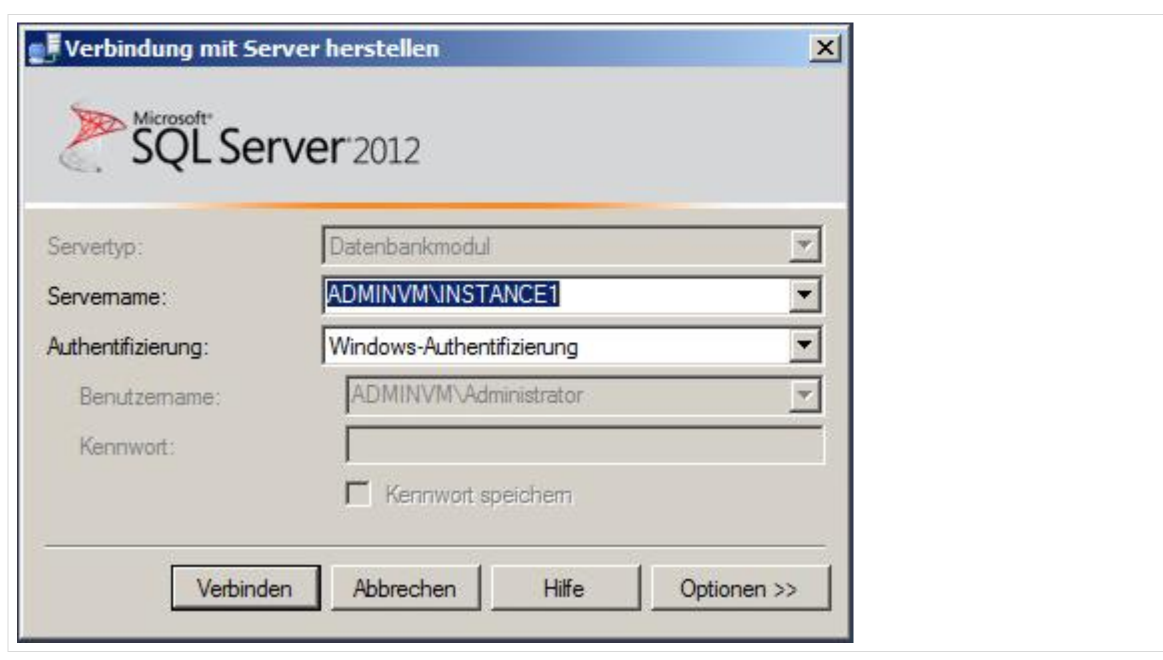


Abb. 200: Verbindung zum SQL-Server aufbauen

Um den Domänen-Administrator zu den Datenbank-Benutzern hinzuzufügen, navigieren Sie im „*Objekt-Explorer*“ auf „*Sicherheit* | *Anmeldungen*“. Drücken Sie auf die rechte Maustaste und wählen Sie den Eintrag „*Neue Anmeldung*“. Es öffnet sich ein neues Fenster.

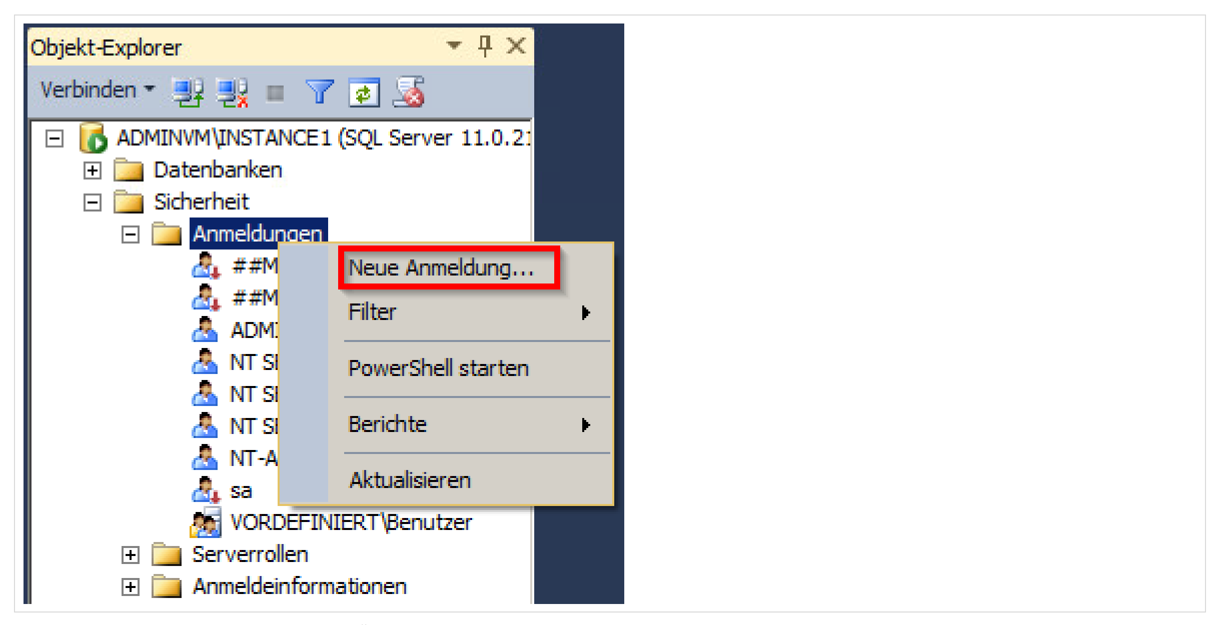


Abb. 201: Eine „neue Anmeldung“ erstellen.

Die folgende Prozedur zum Hinzufügen des Domänenadministrators ist verschachtelt.

Hierzu müssen Sie zunächst im Fenster „*Anmeldung – Neu*" im Reiter „*Allgemein*“ neben dem Feld „*Anmeldename*“ auf „*Suchen*“ klicken (A). Es öffnet sich ein neues Fenster „Benutzer oder Gruppe auswählen“.

Drücken Sie in diesem Fenster zunächst auf den Knopf „*Pfade*“ (B).

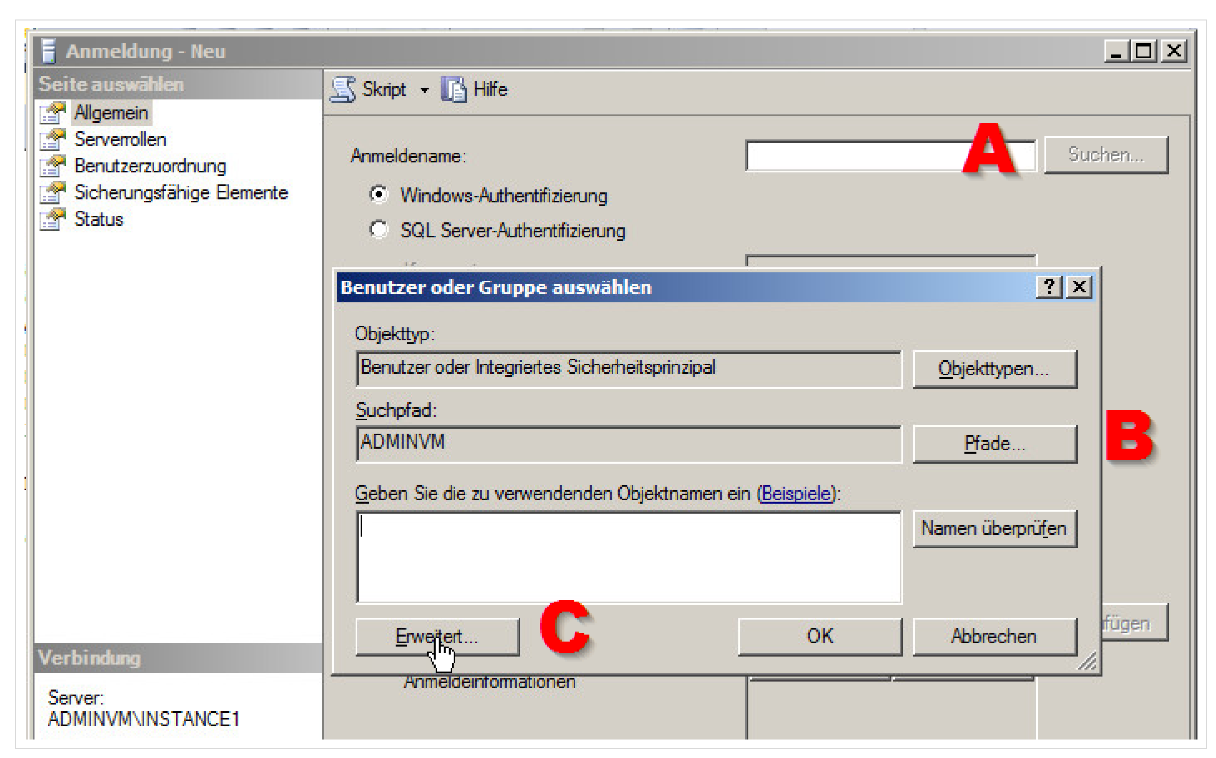


Abb. 202: Anlegen einer neuen Anmeldung

Es öffnet sich ein Dialogfenster „*Windows-Sicherheit*“, in das Sie die Zugangsdaten des Domänen-Administrators eingeben.

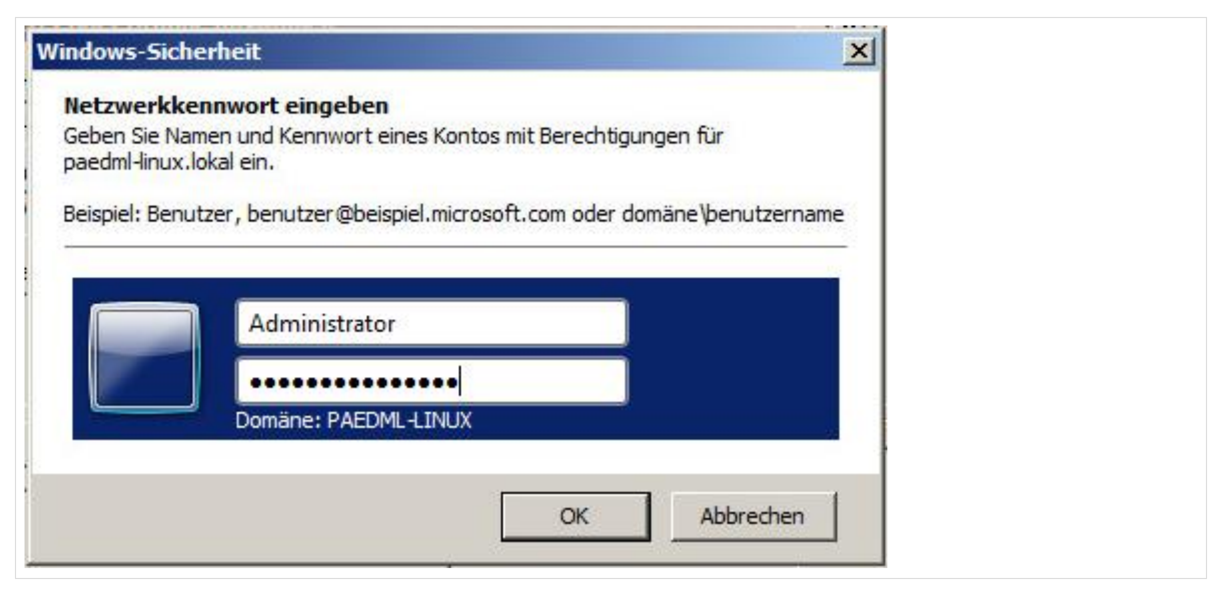


Abb. 203: Anmeldung an der Domäne

Anschließend erhalten Sie ein Dialogfenster, in dem Sie die Schuldomäne auswählen müssen, in der sich der Domänen-Benutzer „Administrator“ befindet. Bestätigen Sie die Auswahl mit „*OK*“.

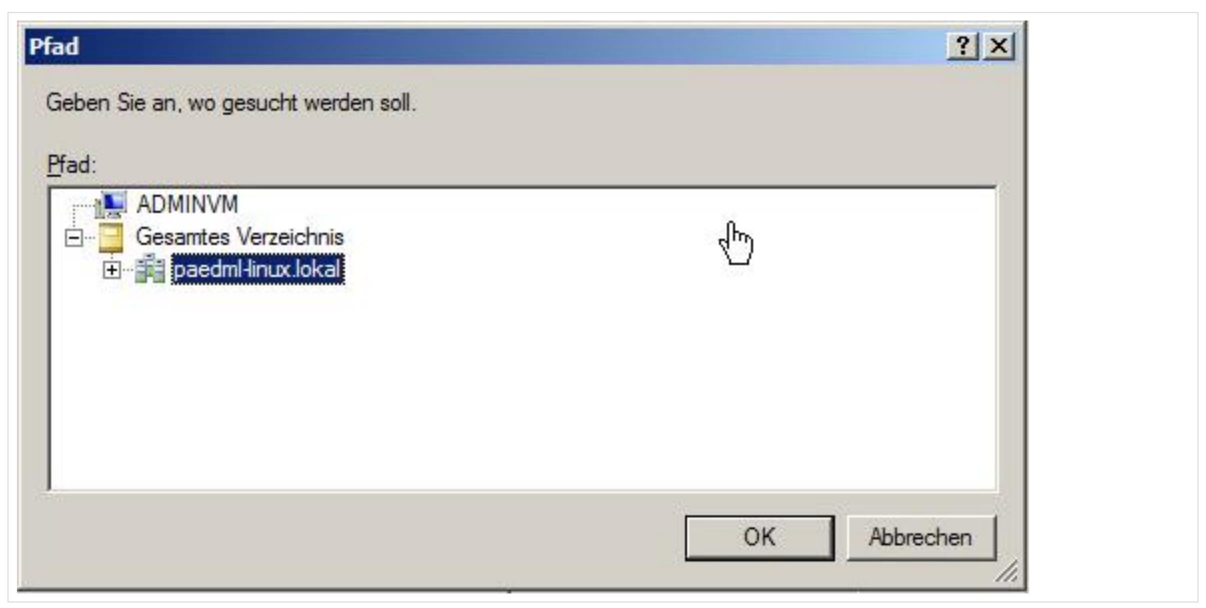


Abb. 204: Auswahl der Domäne

Das vorherige Fenster „*Benutzer oder Gruppe auswählen*“ wird umbenannt nach „*Benutzer, Dienstkonto oder Gruppe auswählen*“. Drücken Sie dort auf „*Erweitert*“ (C).

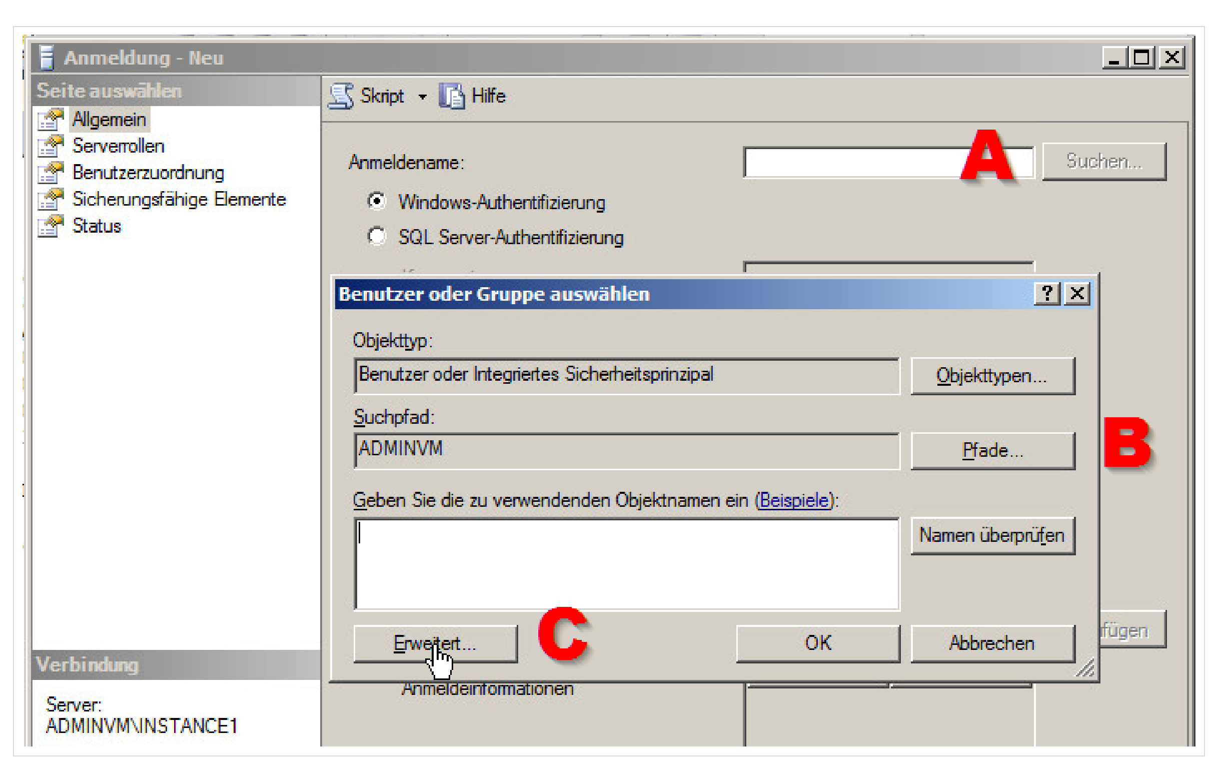


Abb. 205: Anlegen einer neuen Anmeldung

Es öffnet sich ein neuer Dialog. Drücken Sie auf „*Jetzt suchen*“. Der leere Bereich „*Suchergebnisse*“ wird darauf hin befüllt. Wählen Sie den Eintrag „*Administrator*“, der in der Spalte „*Ordner*“ den Namen der Domäne „*paedml-linux.lokal*“ eingetragen hat und bestätigen Sie die Auswahl mit „*OK*“.

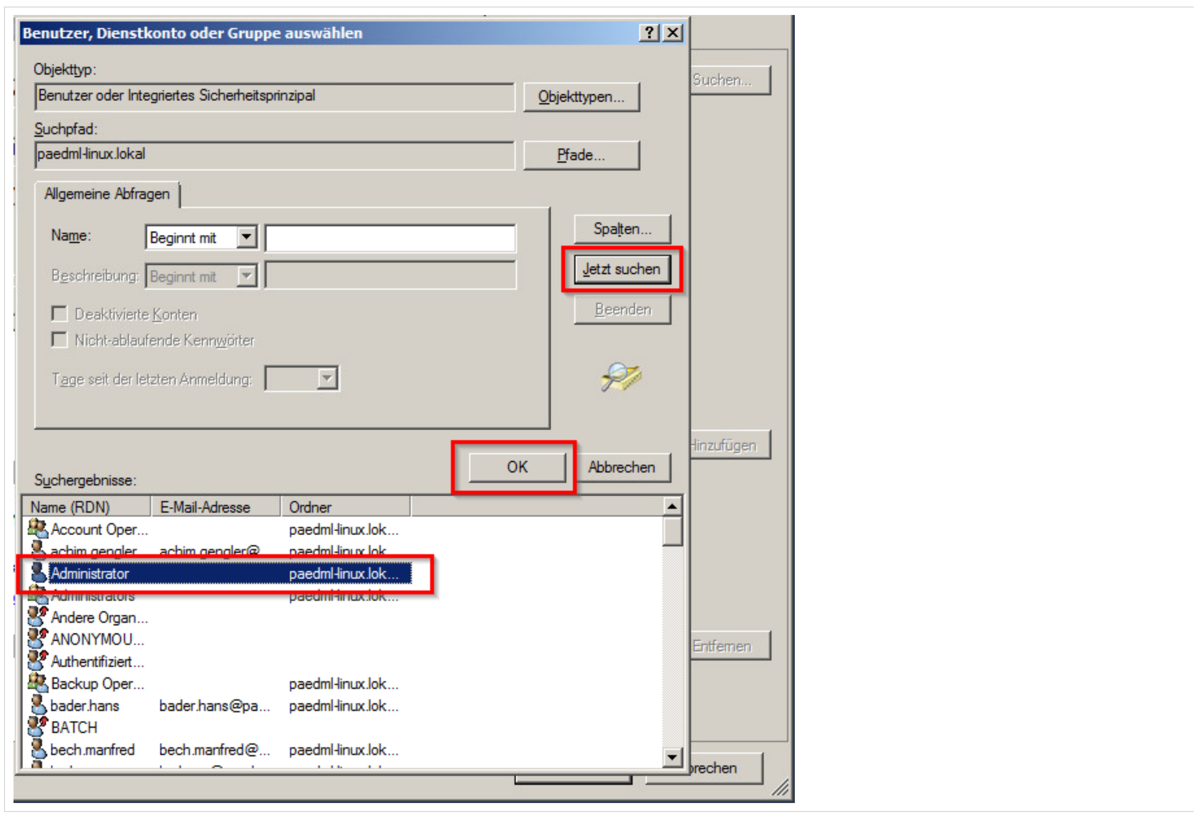


Abb. 206: Neuer Name, gleiches Fenster – Benutzer auswählen

Das nächste Dialogfenster sollte jetzt den „richtigen“ Domänen-Administrator anzeigen (*Administrator@PAEDML-LINUX.LOKAL*). Auch hier wieder mit „*OK*“ bestätigen.

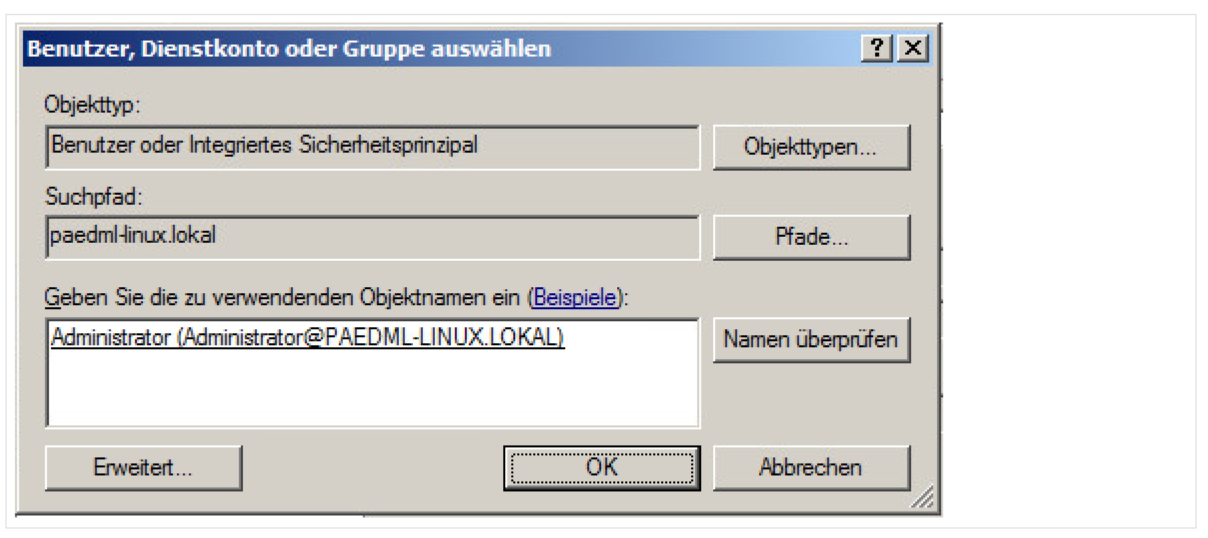


Abb. 207: Bestätigung des Domänenadministrators

Bevor das Profil gespeichert werden kann, müssen Sie dem neuen Benutzer die notwendigen Rechte zuweisen, damit dieser auf die Datenbank zugreifen kann.

Dies geschieht über den Reiter „*Serverrollen*“. Setzen Sie einen Haken bei den Einträgen „*dbcreator*“, „*public*“, „*serveradmin*“ und „*sysadmin*“. Abschließend können Sie den Benutzer anlegen, indem Sie auf „*OK*“ drücken.

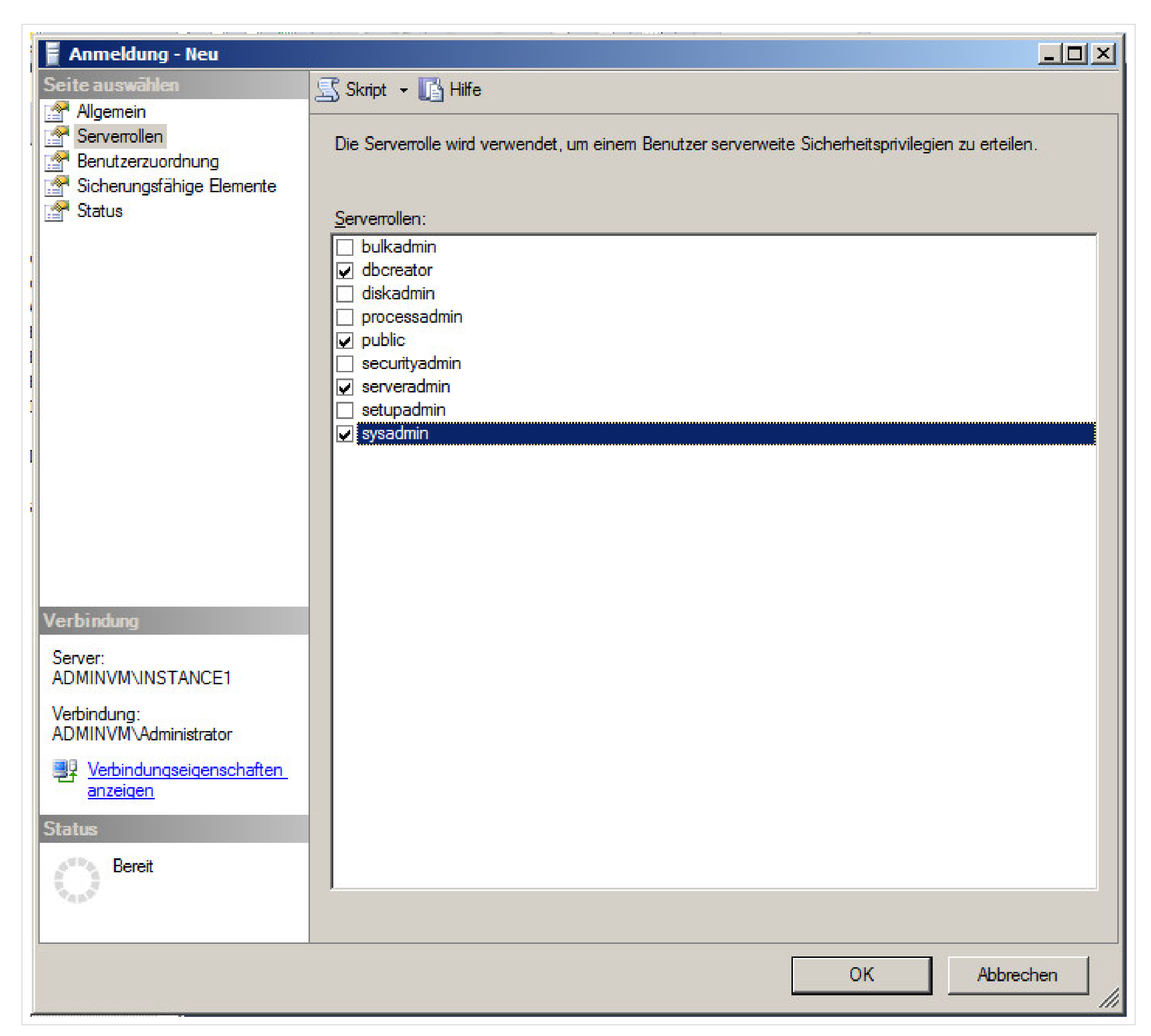


Abb. 208: Zuweisung der Serverrollen

Im Objektexplorer der Datenbank sollte im Anschluss der neue Eintrag „*PAEDML-LINUX\Administrator*“ vorhanden sein.

Das „*SQL Server Management Studio*“ kann nun geschlossen werden.

13.2 Anlegen einer neuen VAMT-Datenbank

Im nächsten Zwischenschritt müssen Sie – immer noch als lokaler Administrator – eine *VAMT-*Datenbank anlegen.

Öffnen Sie hierfür das *Volume Activation Management Tool* (*VAMT*) über das Startmenü.

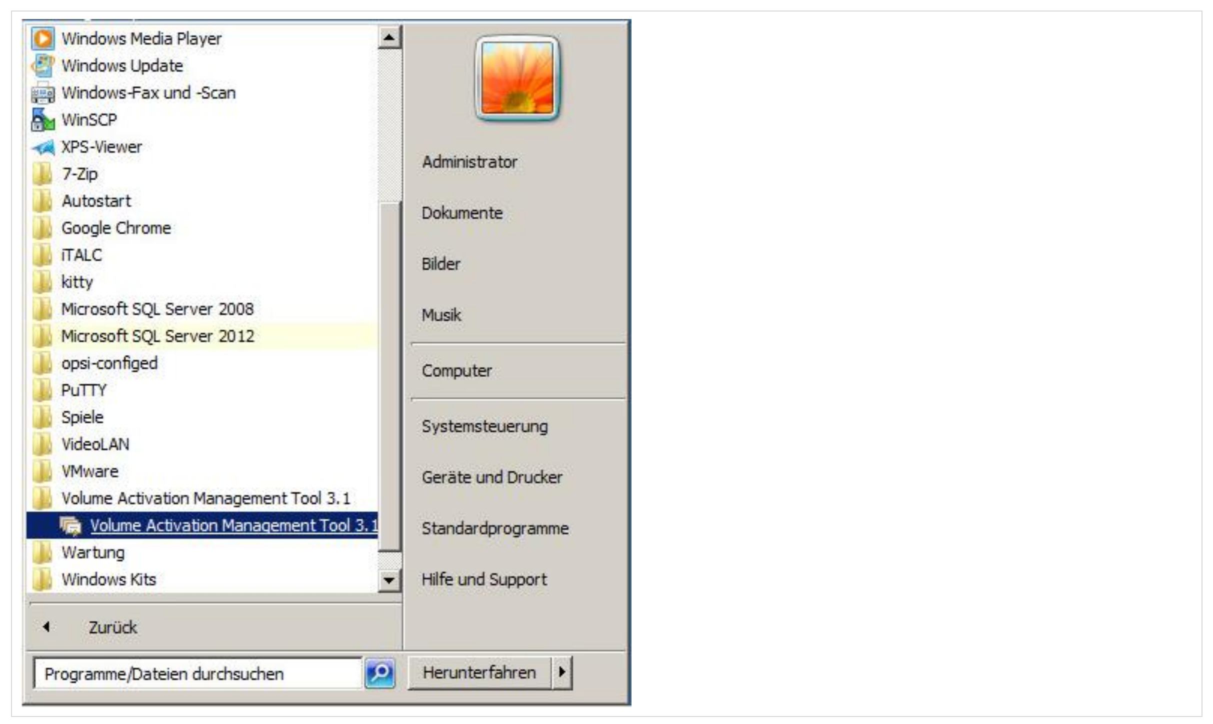


Abb. 209: Aufruf von VAMT über das Startmenü

Beim Aufruf des Programmes werden Sie nach einer Datenbank gefragt, in der die Daten abgelegt werden sollen.

Überprüfen Sie hier, ob im Feld „*Server*“ die lokale Maschine „*ADMINVM\INSTANCE1*“ eingetragen ist. Im Feld „*Database*“ wählen Sie den Eintrag „<Create new Database>“ und als Name tragen Sie im Feld „*New Database Name*“ den Wert „*vamt*“ ein.

Ein Mausklick auf „*Connect*“ legt die neue *VAMT*-Datenbank an.

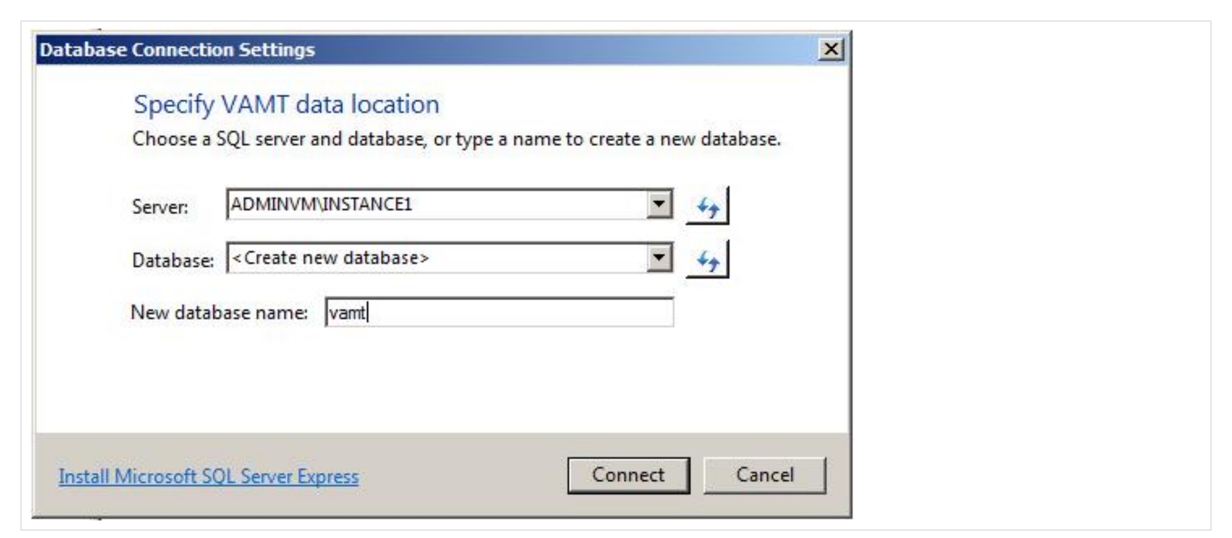


Abb. 210: Anlegen einer neuen Datenbank „vamt“

Die Arbeiten als lokaler Administrator sind hiermit abgeschlossen. Melden Sie sich von *Windows* ab.

13.3 Einrichtung von VAMT

Die Konfiguration von *VAMT* geschieht als Domänen-Administrator. Dieser Benutzer hat – im Gegensatz zum lokalen Administrator – Rechte, um auf die Domäne zuzugreifen.

Mit diesen Rechten kann das Programm die Domäne nach *Microsoft*-Produkten durchsuchen und diese auflisten. Ein händisches Suchen und Eintragen der Produkte wird dadurch umgangen.

Melden Sie sich erneut am Rechner an. Diesmal als *Administrator der Domäne*.



Abb. 211: Anmeldung als Domänen-Administrator

Die Einrichtung der Lizenzverwaltung geschieht in drei Schritten:

1. Durchsuchen des Netzwerkes nach *Microsoft*-Produkten
2. Eingabe der Lizenzschlüssel
3. Aktivierung der Rechner (Kapitel 13.4, Seite 211)

Rufen Sie erneut *VAMT* auf und melden Sie sich an der im vorigen Unterkapitel erstellten Datenbank „*vamt*" an.

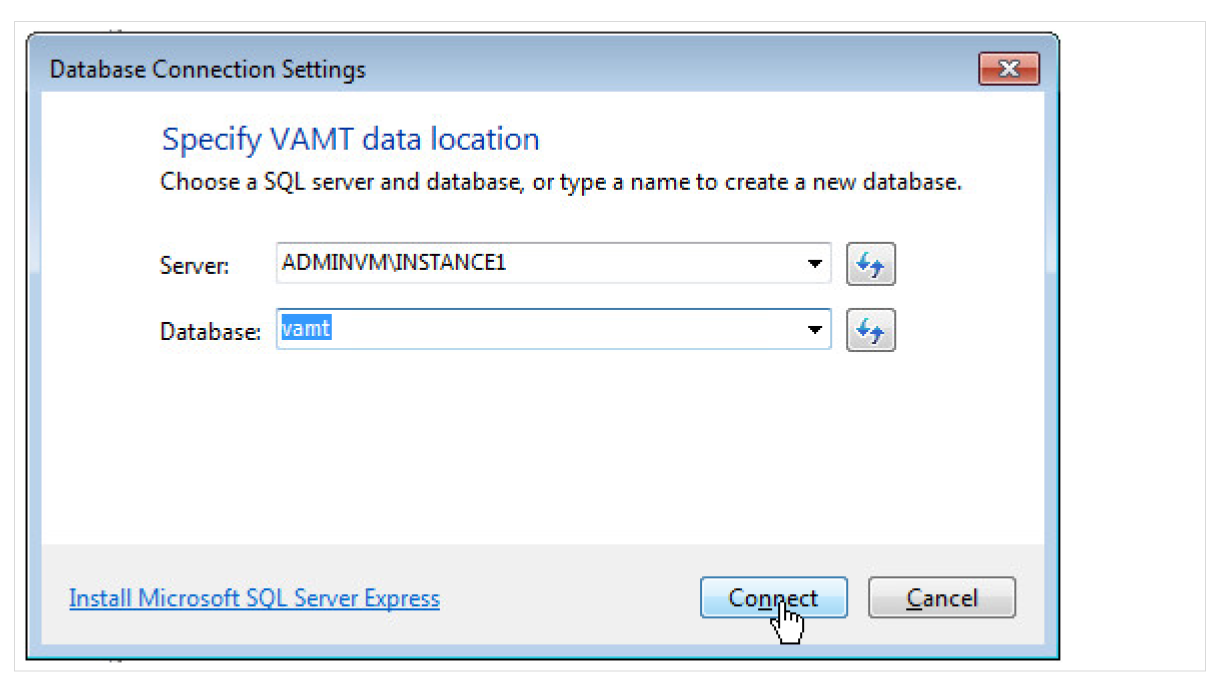


Abb. 212: Anmelden an der Datenbank „vamt"

13.3.1 Suche nach installierten Microsoft-Produkten



Um das Schulnetz nach lizenzpflichtigen *Microsoft*-Produkten zu durchsuchen, müssen alle Rechner, die lizensiert werden sollen, eingeschaltet sein.

Sie können jederzeit weitere Geräte mit dem im Folgenden beschriebenen Verfahren abfragen.

Das *Volume Activation Management Tool* startet beim ersten Aufruf ohne Wissen um die installierten Programme. Dies kann im mittleren Fenster abgelesen werden. Die Einträge unter „*VAMT Inventory*“ und „*Licence overview*“ sind jeweils mit „*0*“ befüllt.

Um das Netzwerk nach Rechnern zu scannen, drücken Sie im linken Bereich des Fensters mit der rechten Maustaste auf den Eintrag „*Products*“ und im Kontextmenü auf „*Discover Products*“.

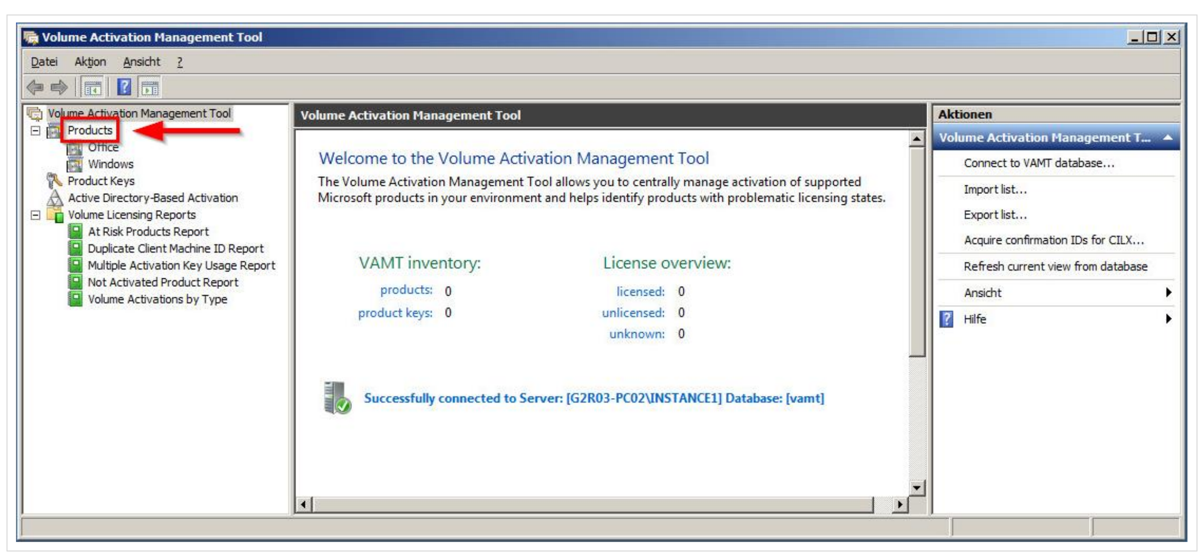


Abb. 213: Erster Aufruf von VAMT

Es geht ein neues Fenster auf. Achten Sie darauf, das die Felder – wie im folgenden Screenshot mit „*Search for computers in the Active Directory*“ und dem Namen der Domäne im Feld „*Search for computers in this domain*“ befüllt sind.

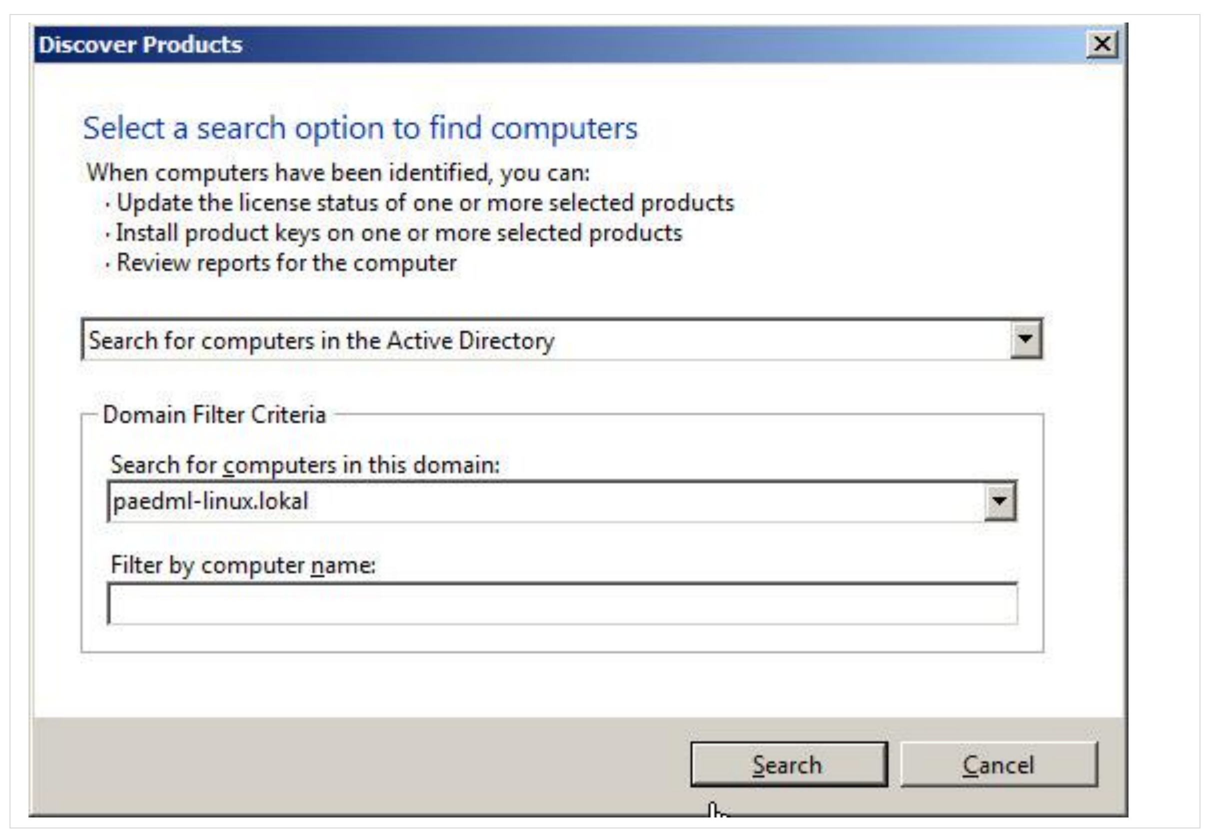
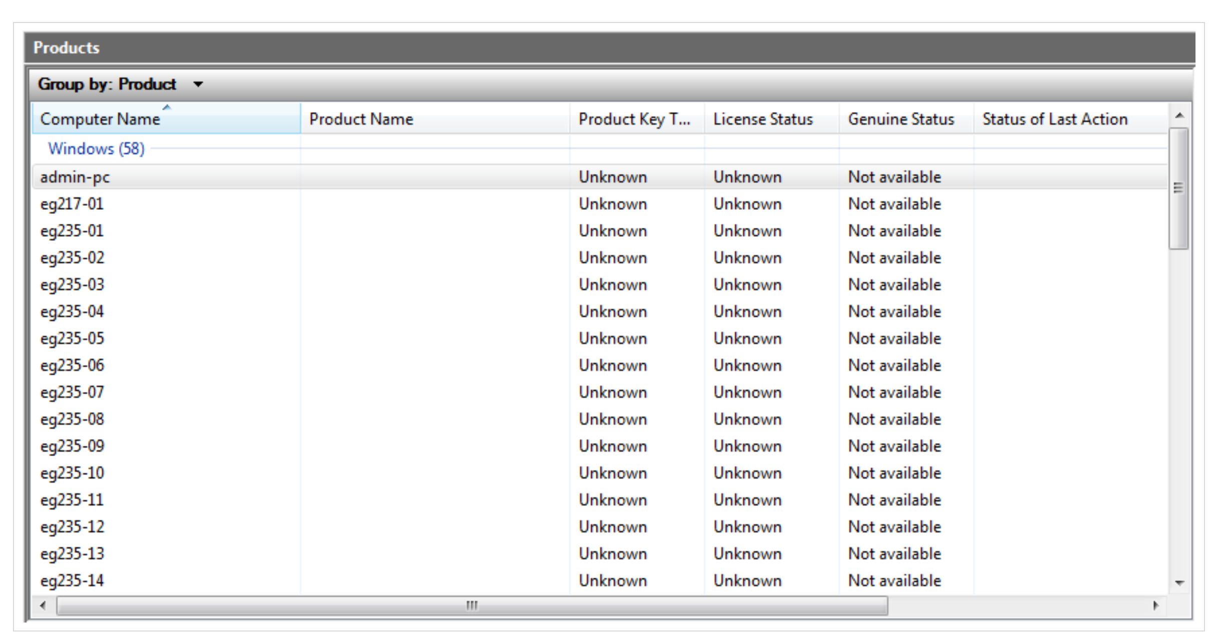


Abb. 214: Suchen nach eingeschalteten Computern

Im mittleren Bereich des *VAMT*-Fensters werden nun die erkannten Rechner angezeigt, wobei noch keine Informationen über die installierten Produkte vorliegen.



Computer Name	Product Name	Product Key T...	License Status	Genuine Status	Status of Last Action
Windows (58)					
admin-pc		Unknown	Unknown	Not available	
eg217-01		Unknown	Unknown	Not available	
eg235-01		Unknown	Unknown	Not available	
eg235-02		Unknown	Unknown	Not available	
eg235-03		Unknown	Unknown	Not available	
eg235-04		Unknown	Unknown	Not available	
eg235-05		Unknown	Unknown	Not available	
eg235-06		Unknown	Unknown	Not available	
eg235-07		Unknown	Unknown	Not available	
eg235-08		Unknown	Unknown	Not available	
eg235-09		Unknown	Unknown	Not available	
eg235-10		Unknown	Unknown	Not available	
eg235-11		Unknown	Unknown	Not available	
eg235-12		Unknown	Unknown	Not available	
eg235-13		Unknown	Unknown	Not available	
eg235-14		Unknown	Unknown	Not available	

Abb. 215: VAMT zeigt nach Suchvorgang alle Rechner der Domäne, die an und somit erreichbar sind

Markieren Sie die Rechnerobjekte und wählen Sie (entweder über das Kontextmenü – mit der rechten Maustaste über markierte Rechner – oder im rechten Bereich des *VAMT*-Fensters) den Eintrag „*Update license status* | *Update current credentials*“.

Sie bekommen anschließend eine Liste der auf den Rechnern installierten *Microsoft*-Produkte angezeigt.

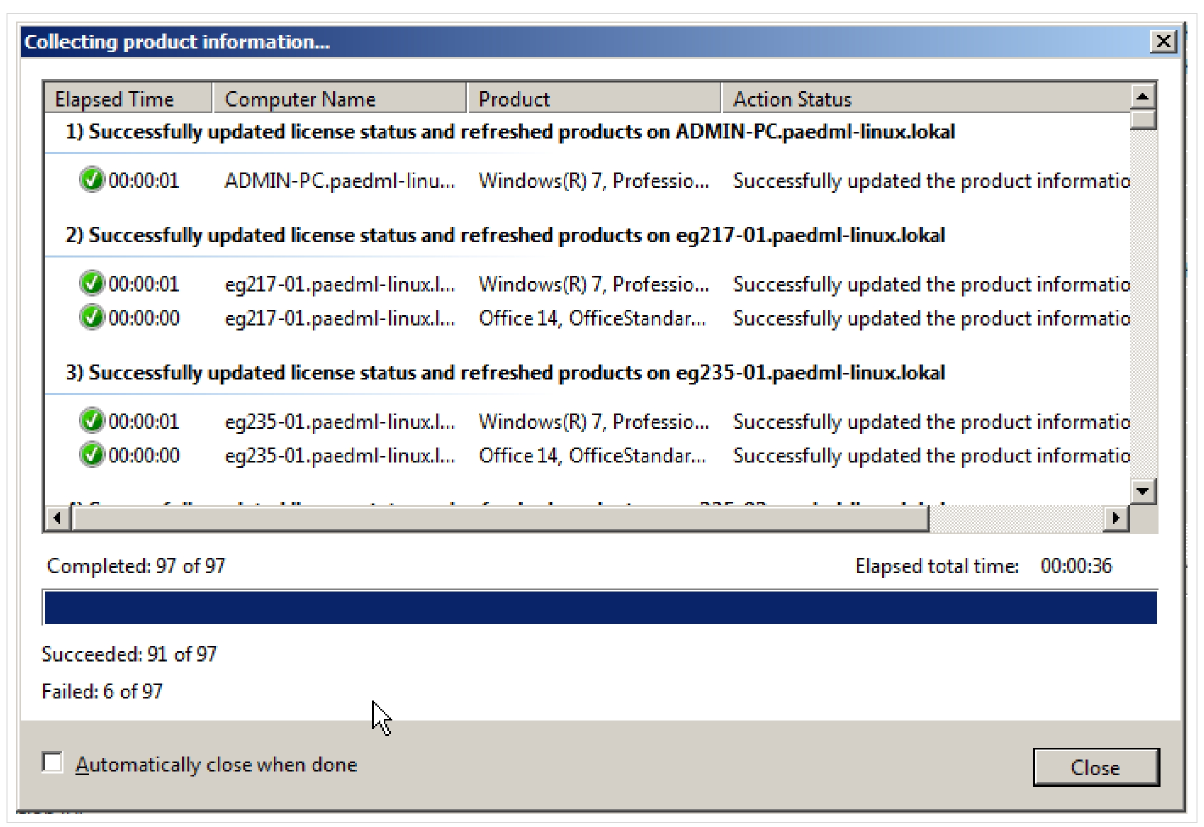


Abb. 216: Anzeige der auf den Rechnern installierten Produkte

Wenn Rechner nicht erreichbar sind, dann erhalten Sie eine Fehlermeldung. Die Nicht-Erreichbarkeit von Rechnern kann verschiedene Ursachen haben:

1. Netzwerkprobleme
2. Der Rechner wurde in der Zwischenzeit heruntergefahren
3. IP-Konflikte.

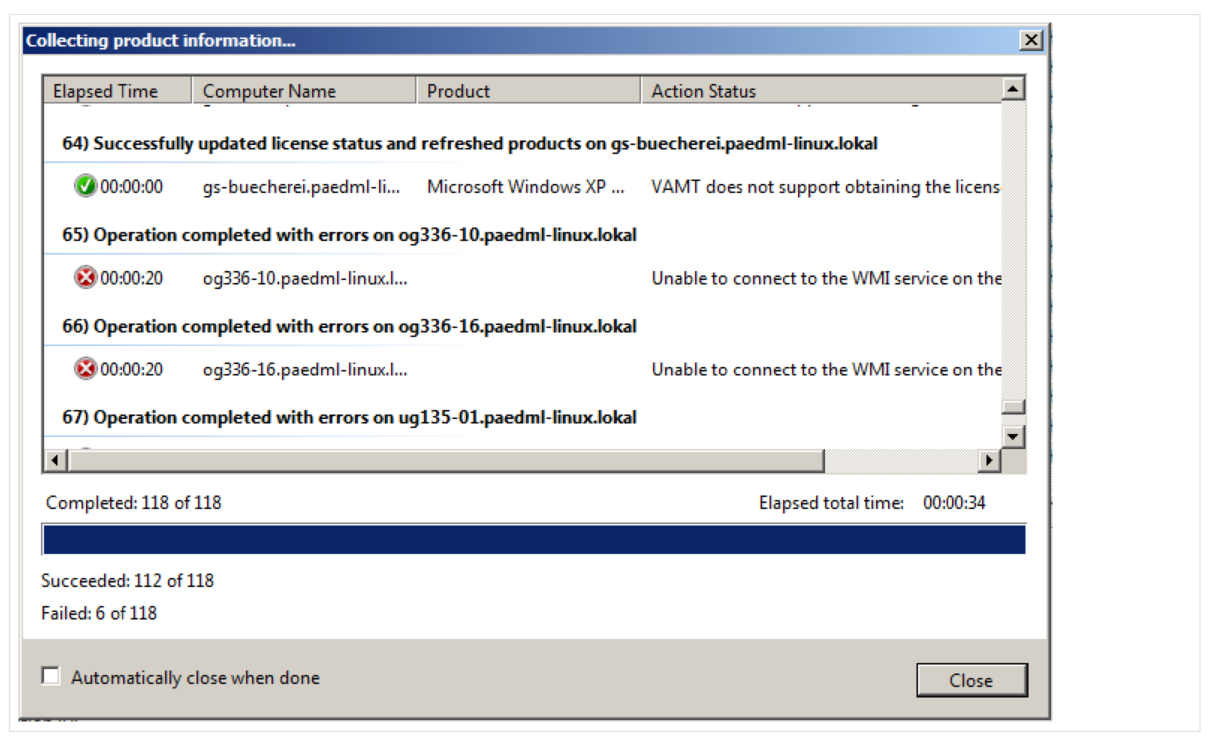


Abb. 217: Nicht erreichbare Rechner werden unten in der Liste angezeigt.

Im Hauptfenster sehen Sie im Feld „*Products* | *Product Details*" (mittlere Spalte) weitere Informationen zu den Clients.

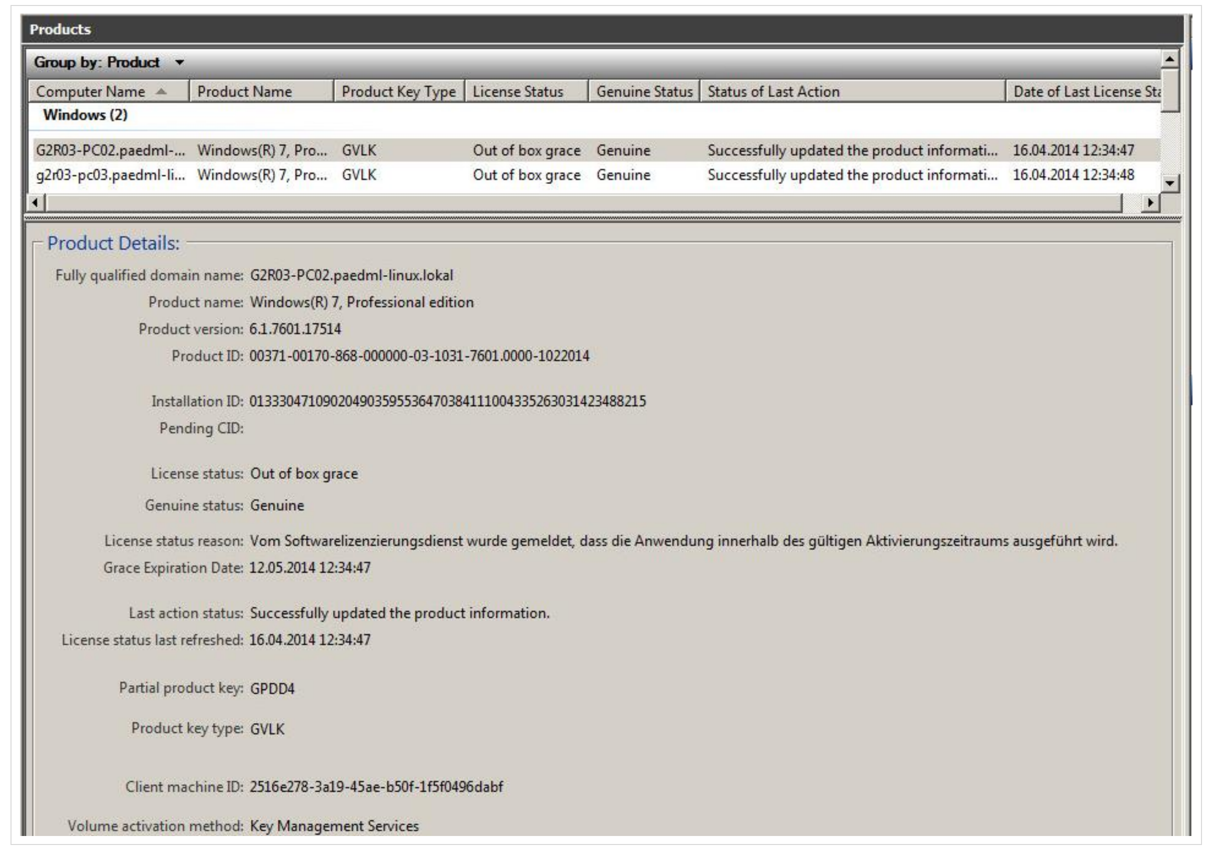


Abb. 218: Details zu den installierten Produkten

Der zentrale Eintrag, um den es in diesem Kapitel geht ist der Eintrag in der Spalte „*License Status*“, der im vorliegenden Beispiel mit „*Out of box grace*“ befüllt ist. „*Out of box grace*“ steht für die Kulanzfrist, in der der Rechner ohne Aktivierung betrieben werden kann.

13.3.2 Eingabe der Lizenzschlüssel

Nachdem nun die Produktinformationen gesammelt wurden, können Sie Ihre Lizenzschlüssel eingeben.

Dies geschieht über den Menüpunkt „*Product Keys*“ im linken Feld des *VAMT*-Fensters. Aktivieren Sie diesen Eintrag und klicken Sie entweder mit der rechten Maustaste darauf oder wählen Sie im linken Bereich des Fensters den Menüpunkt „*Add Product Keys*“.

Es öffnet sich ein neues Fenster, in dem Sie einen oder mehrere Lizenzschlüssel untereinander eingeben können. Bestätigen Sie die Eingabe mit „*Add Key(s)*“.

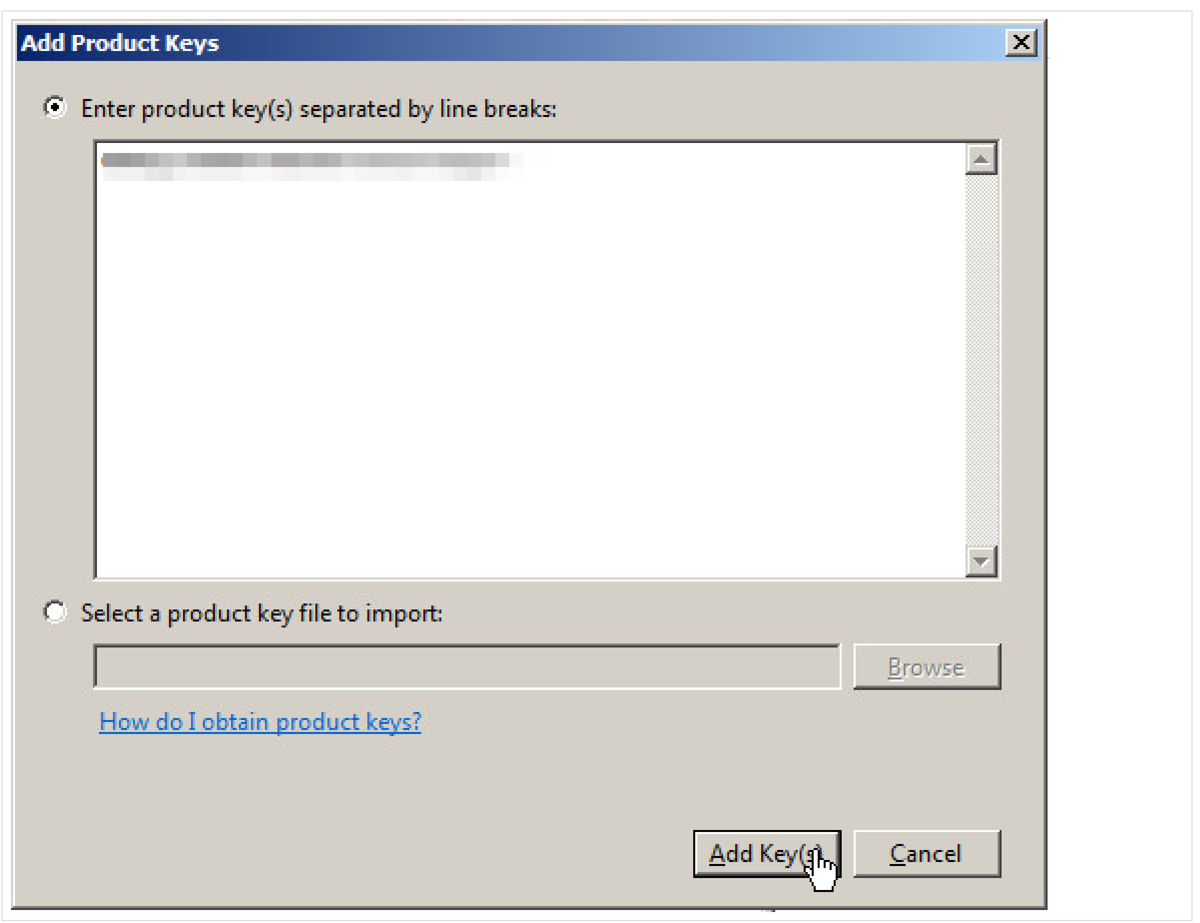


Abb. 219: Eingabe der Lizenzschlüssel

Die Lizenzschlüssel werden bei *Microsoft* auf Gültigkeit überprüft und – sofern diese Überprüfung erfolgreich ist – in *VAMT* hinterlegt. Sie sehen im Anschluss im vorher leeren Feld „*Product Keys*“ Informationen zu den eingetragenen Lizenzschlüsseln.

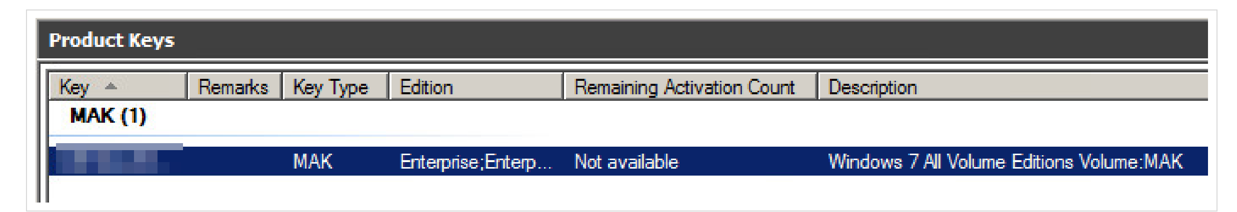


Abb. 220: Informationen zum Lizenzschlüssel – ohne Angabe über verbleibende Aktivierungen

Die Spalte „*Remaining Activation Count*" zeigt an, wie oft der eingegebene Schlüssel noch aktiviert werden kann. Sollte hier kein Wert eingetragen sein, können Sie mit der rechten Maustaste und dem Eintrag „*Refresh product key data online*" die Lizenzinformationen aktualisieren.

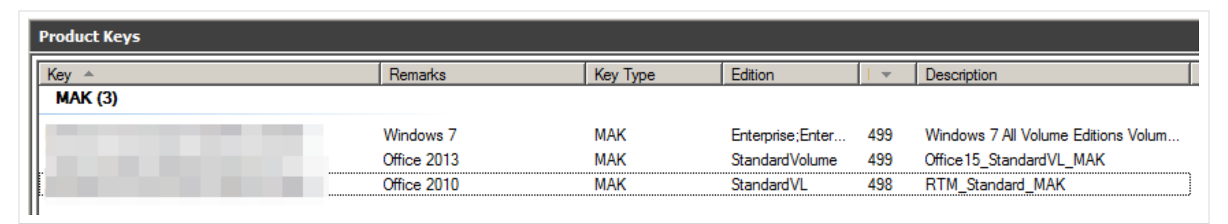


Abb. 221: Informationen zum Lizenzschlüssel – mit Angabe über verbleibende Aktivierungen

Hinweis zu Fehlermeldungen beim Abruf von Lizenzinformationen

Wenn Sie Fehlermeldungen bekommen, die besagen, dass keine Verbindung zu *Microsoft* hergestellt werden kann, um den Lizensierungsstatus abzurufen, überprüfen Sie die „*Internetoptionen*" in der „*Systemsteuerung*".

Im Reiter „*Verbindungen*" klicken Sie auf „*LAN-Einstellungen*". Dort müssen alle Haken deaktiviert sein (vgl. folgender Screenshot).

Dies funktioniert nur bei der *AdminVM***, da für dieses Gerät eine Weiterleitung in der Firewall eingerichtet ist.** (Menüpunkt „*Firewall* | *Rules*", Reiter „*PAEDAGOGIK*")

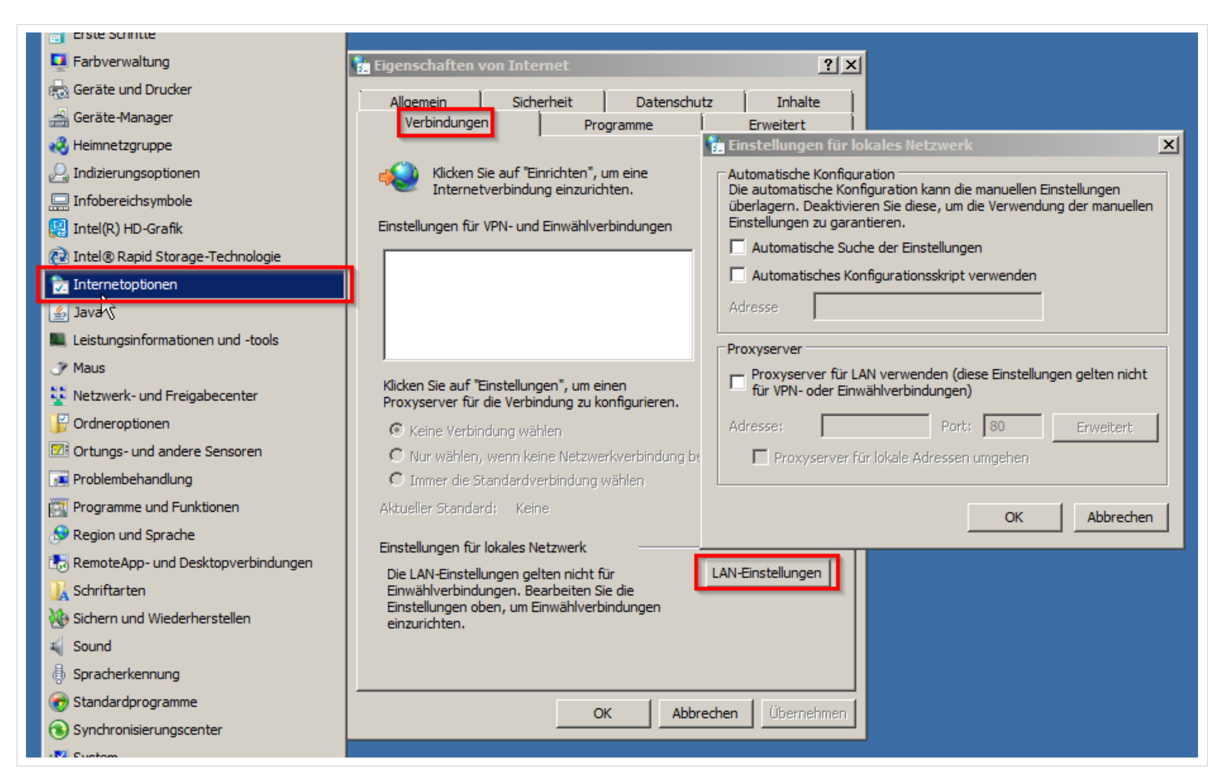


Abb. 222: Deaktivierung des Proxy-Servers

13.4Aktivierung der Lizenzen

Nachdem wir nun zunächst die Informationen über die Rechner gesammelt und anschließend unsere Lizenzschlüssel hinterlegt haben, geht es darum die beiden zu verheiraten und unsere Software zu lizensieren.

Ein frisch installierter Rechner ist erwartungsgemäß nicht aktiviert. Dies können Sie am *Windows*-Rechner überprüfen, indem Sie über den *Windows*-Button das Fenster „*Start* | *Systemsteuerung* | *System*" aufrufen.

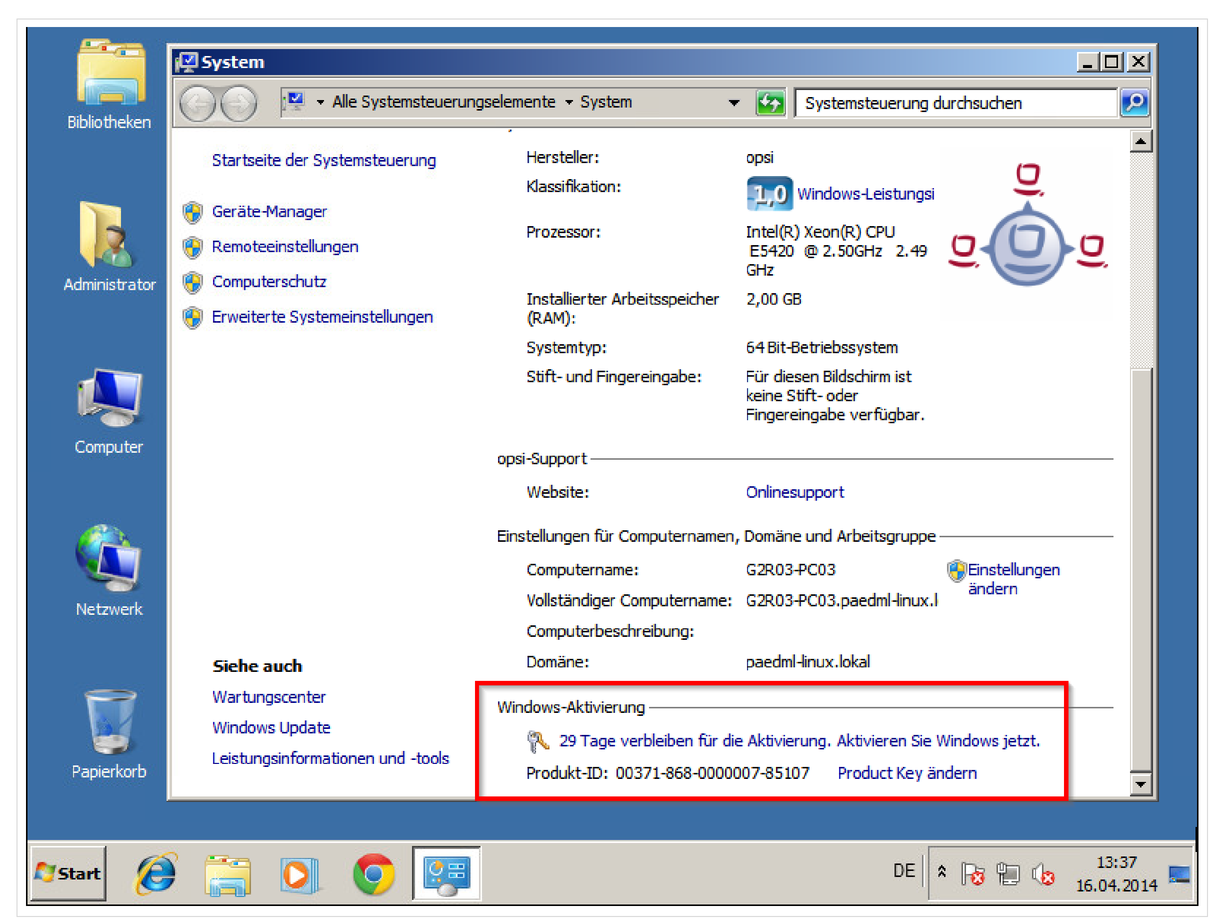


Abb. 223: Windows *in der „Duldungsphase“*

Um die Lizenz auf den Rechnern auszuspielen, wählen Sie im linken Fenster von *VAMT* den Menüpunkt „*Products*“ und wählen Sie die zu aktivierenden Maschinen. Mit dem Eintrag „*Install Product Key*“ (rechte Maustaste oder Einträge im rechten Bereich des Fensters) können Sie den ausgewählten Rechnern einen Produktschlüssel zuweisen. Drücken Sie auf „*Install Product Key*“, um den Schlüssel zu verteilen.

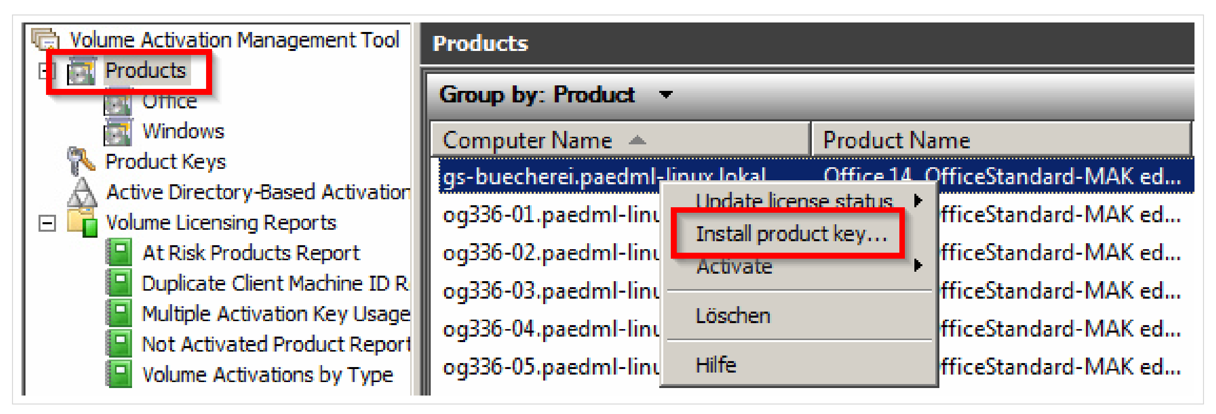


Abb. 224: Zuweisung eines Lizenzschlüssels

Es öffnet sich ein Fenster mit den im System hinterlegten Lizenzschlüsseln. Hier müssen Sie den Schlüssel wählen, den Sie auf den Rechner ausspielen wollen. Es kann immer nur ein Schlüssel ausgespielt werden. Daher muss der Vorgang für Betriebssystem und Office-Programm getrennt voneinander ausgeführt werden.

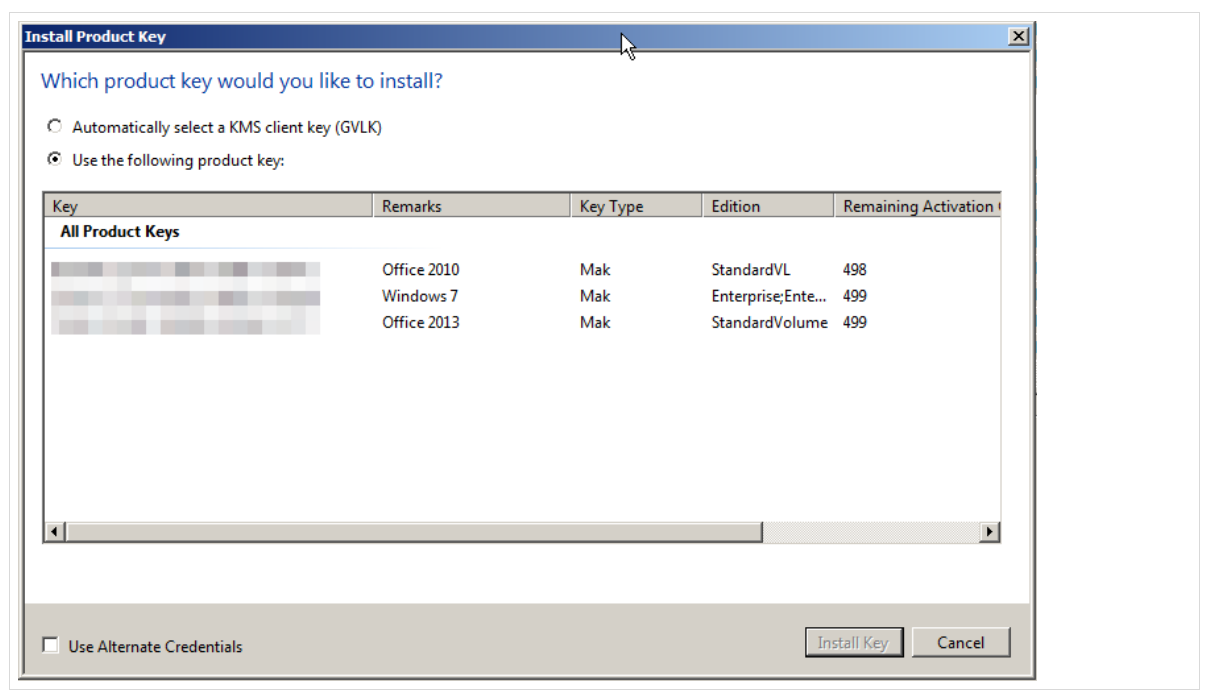


Abb. 225: Auswahl des Lizenzschlüssels

Wählen Sie das Produkt, das Sie installieren wollen und drücken Sie auf „*Install Key*“.

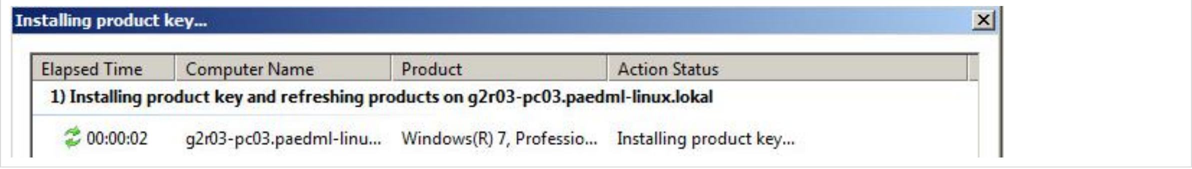


Abb. 226: Der Schlüssel wird …

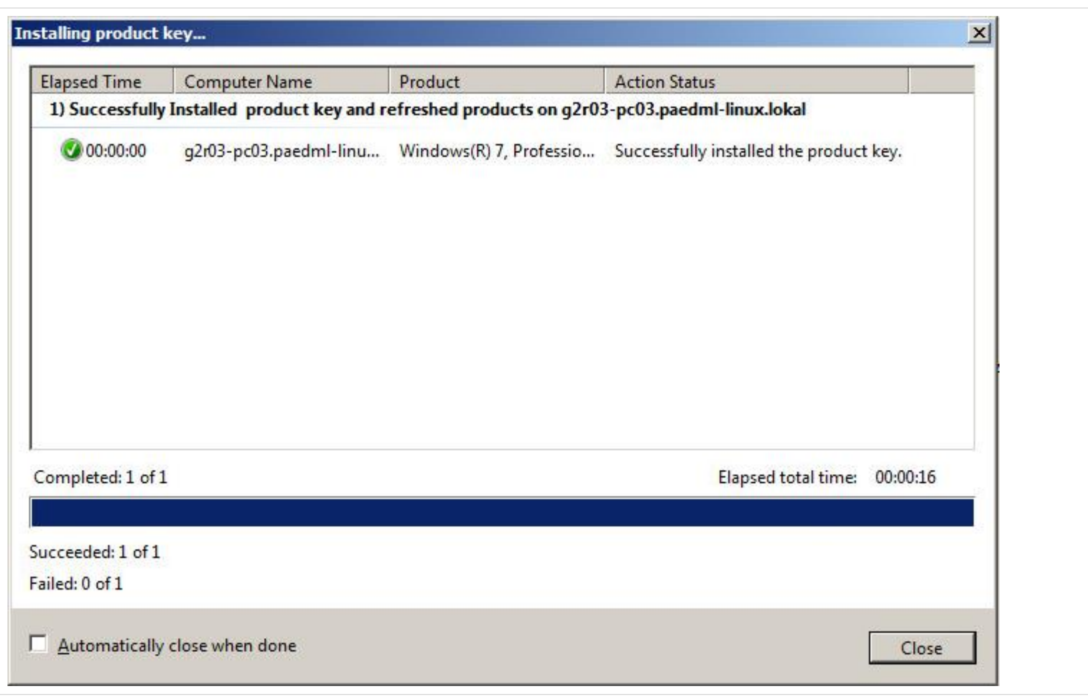


Abb. 227: … auf dem Rechner installiert.

Nun ist der Lizenzschlüssel auf den Rechnern hinterlegt und muss im letzten Schritt nur noch aktiviert werden. Hierfür sind wiederum die zu aktivierenden Rechner zu markieren und mit dem Kontextmenü der rechten Maustaste ist der Eintrag *„Activate* | *Proxy activate*“ zu wählen.

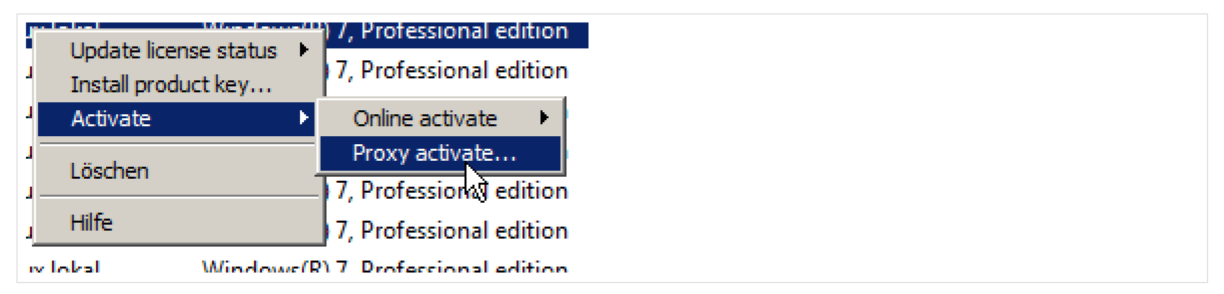


Abb. 228: Aktivierung über Proxy

Im nächsten Dialog werden Sie gefragt, ob Sie die Aktivierungsinformationen nur herunterladen oder das Gerät auch gleich aktivieren wollen. Wir empfehlen Ihnen die Aktivierung gleich durchzuführen. Hierfür muss das Optionsfeld *„Aquire confimation ID, apply to selected machine(s) and activate*“ ausgewählt werden.

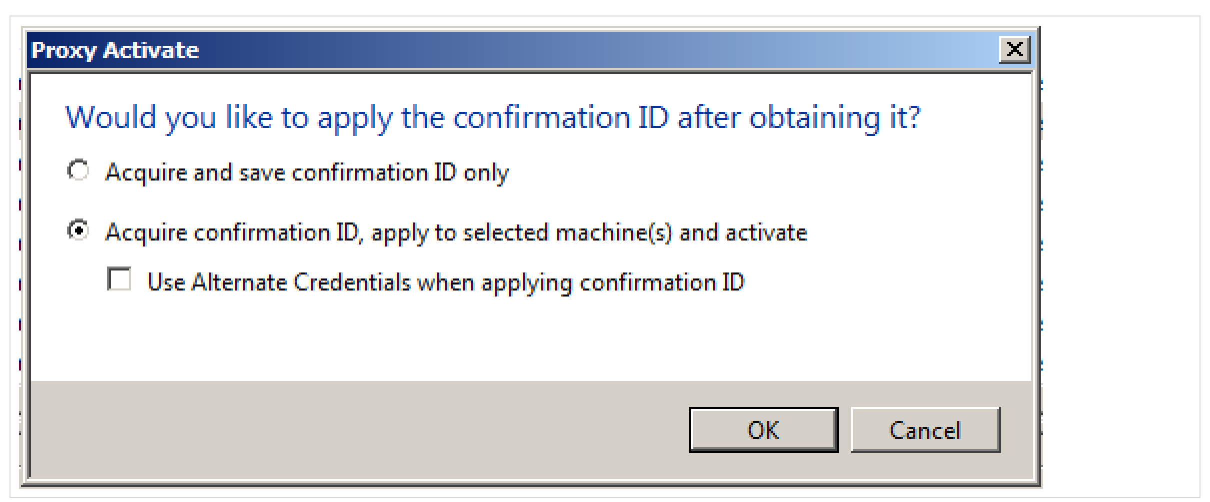


Abb. 229: Soll das die Software gleich aktiviert werden?

Wenn Sie auf *„OK*“ drücken fragt das Programm zunächst nach einer *„confirmation Id*“ (Bestätigung), die auf den Rechner ausgespielt wird.

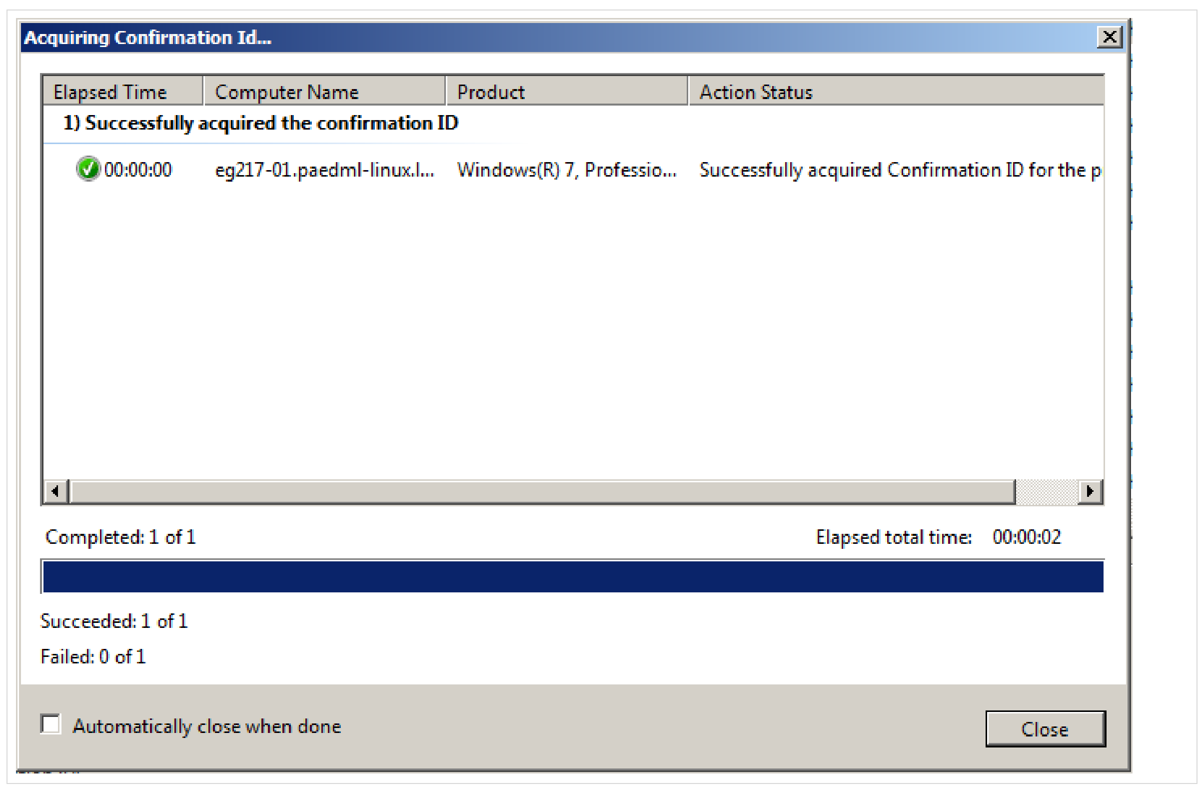


Abb. 230: Ausspielen der Bestätigungs-ID

Nach erfolgreicher Bestätigung wird die Lizenz im nächsten Schritt aktiviert.

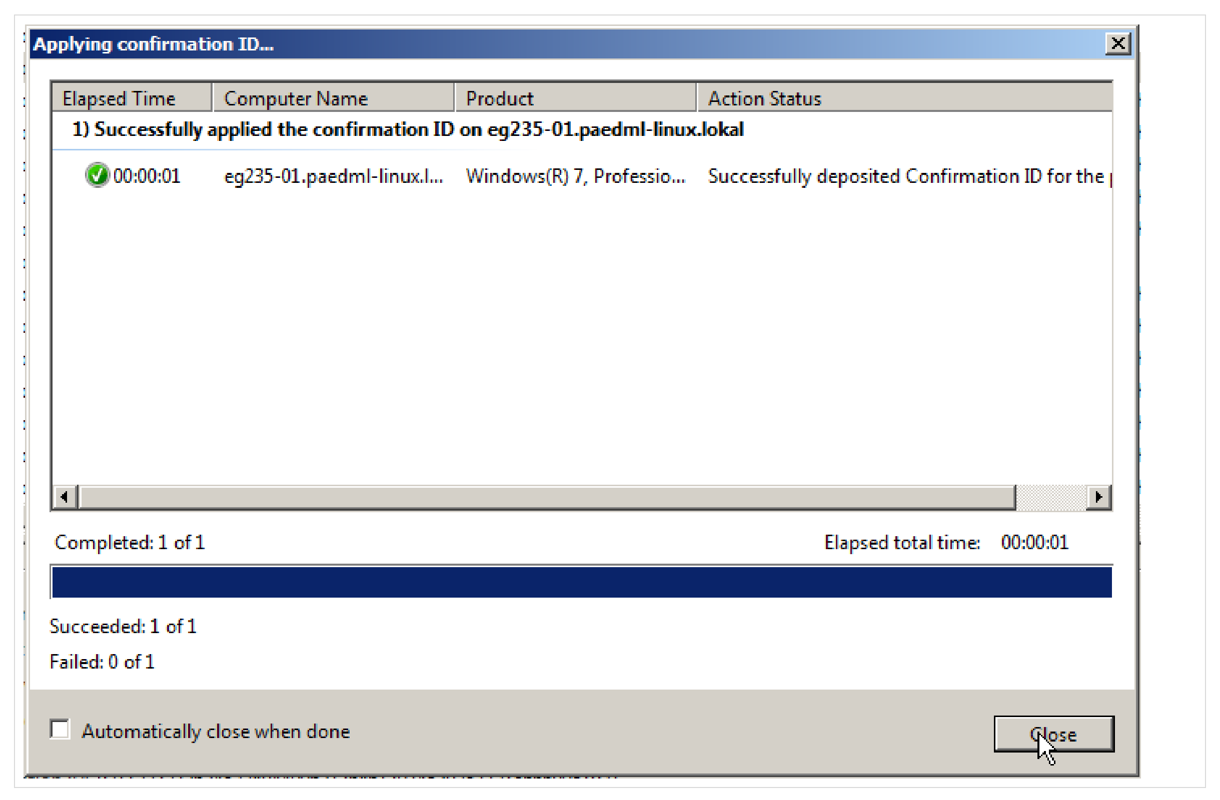


Abb. 231: Aktivierung der Lizenz

Sollte der zweite Schritt fehlschlagen, kann er auch manuell angestoßen werden über die rechte Maustaste „*Activate* | *Apply confimation ID* | *Current credential*“.

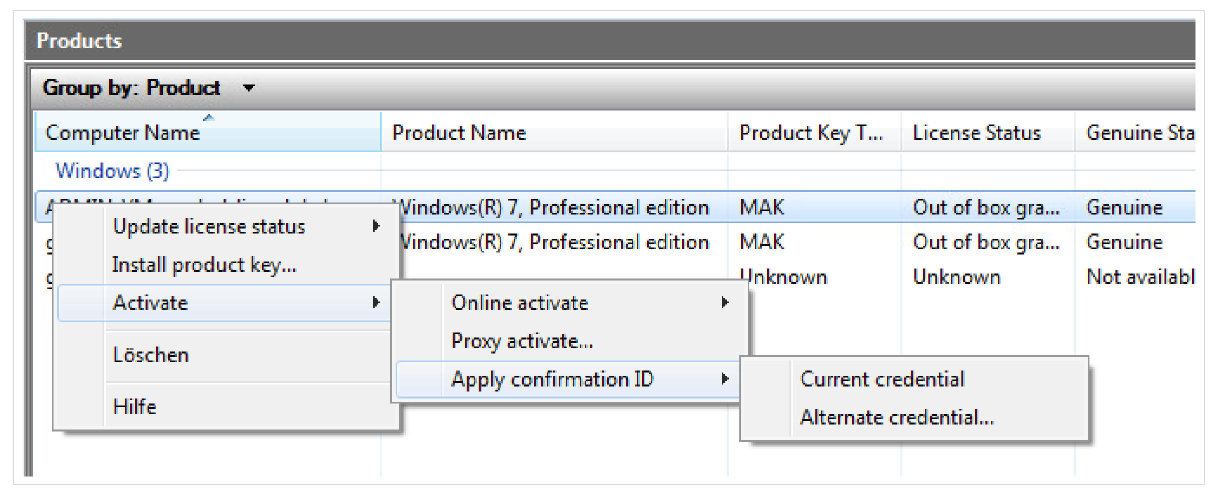


Abb. 232: Manuelle Aktivierung

Nach dem Aktivieren ist der Rechner in der Produktliste mit dem „*Licence Status*“ „*Licensed*“ versehen.

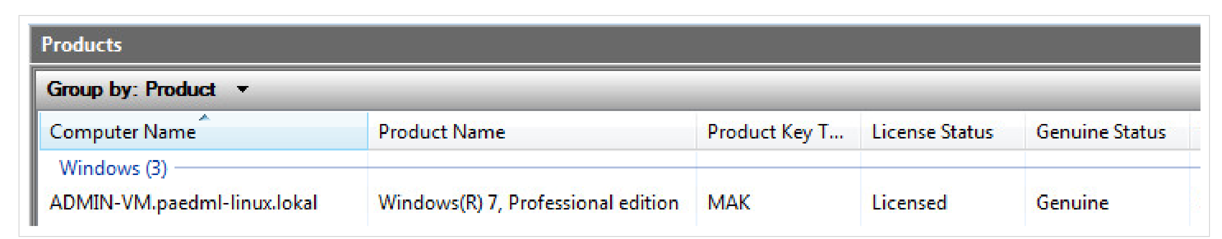


Abb. 233: In der Übersicht ist der Rechner mit dem Lizenzstatus „licensed“ versehen.

Überprüfen Sie die Aktivierung, in dem Sie über den *Windows*-Button das Fenster „*Start* | *Systemsteuerung* | *System*“ aufrufen.

Der Eintrag *Windows*-Aktivierung sollte nun anzeigen, dass *Windows* aktiviert ist.

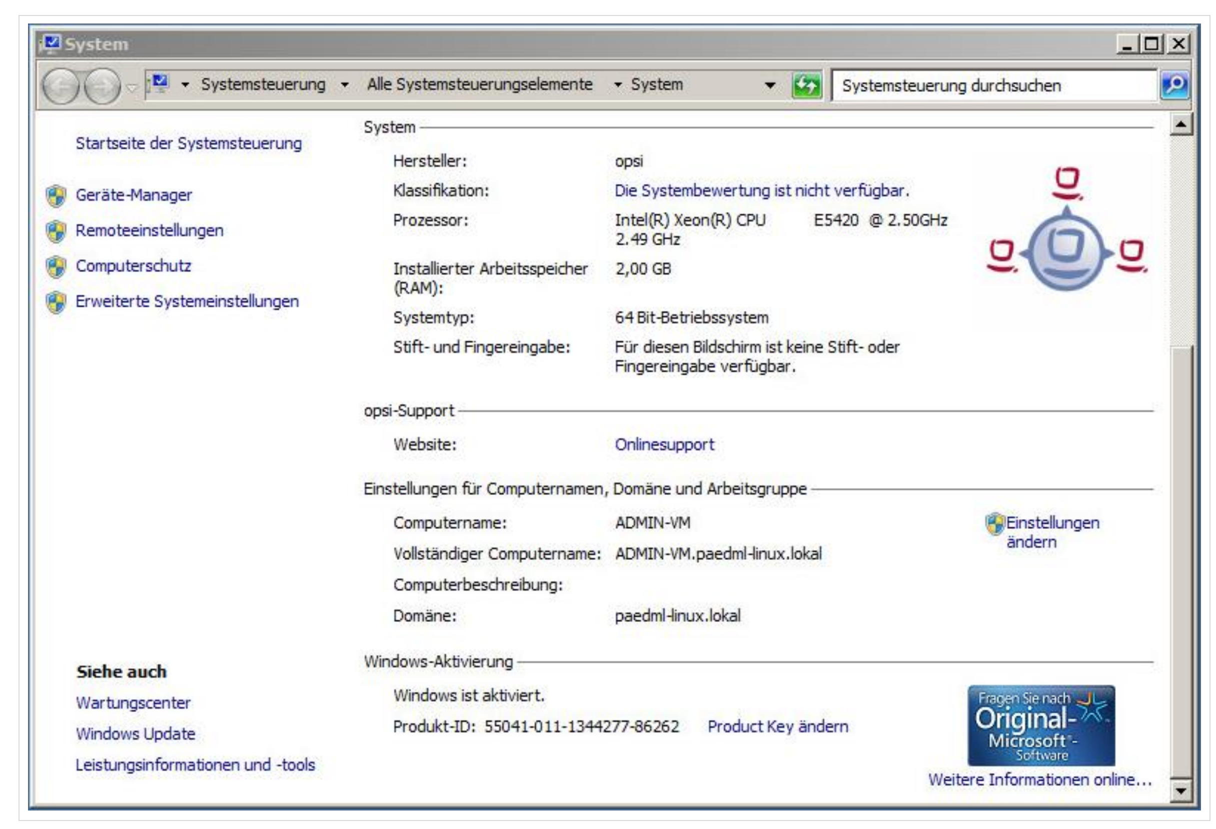


Abb. 234: Windows *wurde aktiviert*

Die Aktivierung von *Microsoft-Office 2010* können Sie über den Reiter „*Datei*“ und dort den Eintrag „*Hilfe*“ überprüfen. Wenn die Aktivierung erfolgreich war, gibt es dort den Eintrag „*Produkt aktiviert*“.



Abb. 235: Office im aktivierten Zustand

13.5 Sicherung der Lizenzinformationen

13.5.1 Sicherung über ein lokales Image auf den Rechnern

Die Aktivierung der Clients sollte nun nach Möglichkeit in lokalen Images auf den Rechnern gespeichert werden. Hierfür sollten je Maschine die folgenden Schritte durchgeführt werden:

1. Installation des Rechners
2. Aktivierung der Lizenz auf dem Gerät
3. Erstellung eines lokalen Images wie in Kapitel 9 ab Seite 167 beschrieben

Anschließend können Sie den Rechner jederzeit aus dem lokalen Image wieder herstellen, ohne dass die Lizenzinformationen verloren gehen.

13.5.2 Sicherung der Lizenzinformationen von VAMT

Die Lizenzinformationen von *VAMT* können Sie in eine Textdatei exportieren und später – im Fall einer defekten *AdminVM* – in eine neue *VAMT*-Instanz importieren.

Öffnen Sie hierfür in der Menüleiste von *VAMT* den Eintrag „*Aktion* | *Export List*".

In dem sich neu öffnenden Fenster müssen Sie einen Namen für die Sicherungsdatei (im vorliegenden Beispiel: „paedml-Lizenzen") eingeben. Sie können den Sicherungspfad anpassen.

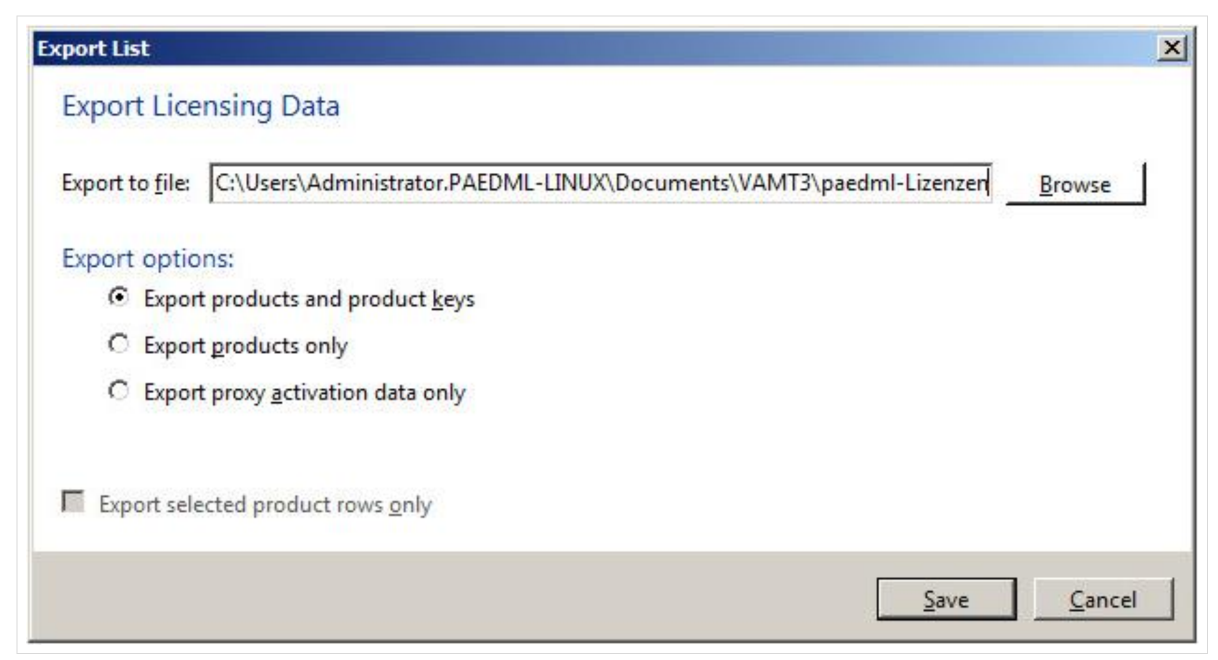


Abb. 236: Wohin sollen die Lizenzdaten gesichert werden?

Die Datei wird im „*.cilx"-Format gespeichert und kann per Mausklick in eine bestehende VAMT-Instanz übertragen werden.

Sichern Sie diese Datei auf einem externen Datenträger!

13.6 Reaktivierung von Lizenzen nach Neuaufsetzen

Wie oben beschrieben, wird empfohlen, dass Sie nach der Aktivierung eines Clients ein Image erstellen. Dadurch werden die Lizenzinformationen in das Image des jeweiligen Rechners geschrieben und sind nach der Imagewiederherstellung verfügbar.

Eine Reaktivierung von Lizenzen ist nur notwendig, wenn Clients neu installiert – anstatt vom lokalen Image wiederhergestellt – wurden.



Voraussetzung für die Reaktivierung ist, dass sich die Hardware der Clients nicht geändert hat.

Microsoft überprüft anhand von Rechnermerkmalen, an welches Gerät eine Lizenz gebunden wird. Geänderte Hardware (z.B. eine andere Festplatte) führt unter Umständen dazu, dass die Lizenz nicht mehr für das Gerät gültig ist.

Die Reaktivierung beim MAK-Aktivierungs-Verfahren geschieht nicht automatisch, sondern muss manuell ausgeführt werden. Das Verfahren ist ähnlich dem der Erstaktivierung.

Hierfür ist als Domänen-Administrator das *Volume Activation Management Tool* (*VAMT*) zu starten und die Datenbank mit den Lizenzdaten zu öffnen.

Wählen Sie anschließend die zu reaktivierenden Clients aus und öffnen Sie das Kontextmenü mit der rechten Maustaste.

Die folgenden Schritte sind nacheinander auszuführen:

1. „*Update license status* | *Current credential*“
   Hiermit wird der Rechner nach installierten *Microsoft*-Produkten untersucht.

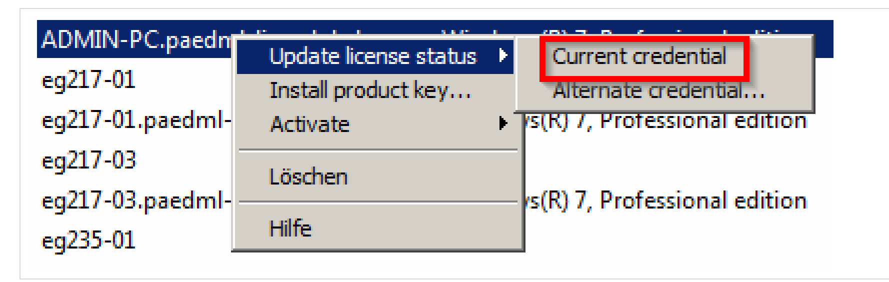


Abb. 237: Erster Schritt der Reaktivierung

2. „*Install product key*“

Nachdem die Lizenzinformationen für den Rechner abgefragt wurden, installieren Sie den Produkt-Schlüssel. Für diesen Schritt muss der Client erneut ausgewählt und mit der rechten Maustaste bearbeitet werden. Mit dem Eintrag „*Install product key…*“ werden die Lizenz-Daten auf den Rechner überspielt.

3. „*Activate* | *Apply confirmation ID* | *Current credential*“

Im letzten Schritt (der nur möglich ist, wenn das Gerät bereits aktiviert war – andernfalls ist der Menü-Eintrag nicht verfügbar) wird der Rechner (erneut) aktiviert. Dabei wird die bestehende Lizenz verwendet und der Lizenzzähler nicht erhöht.

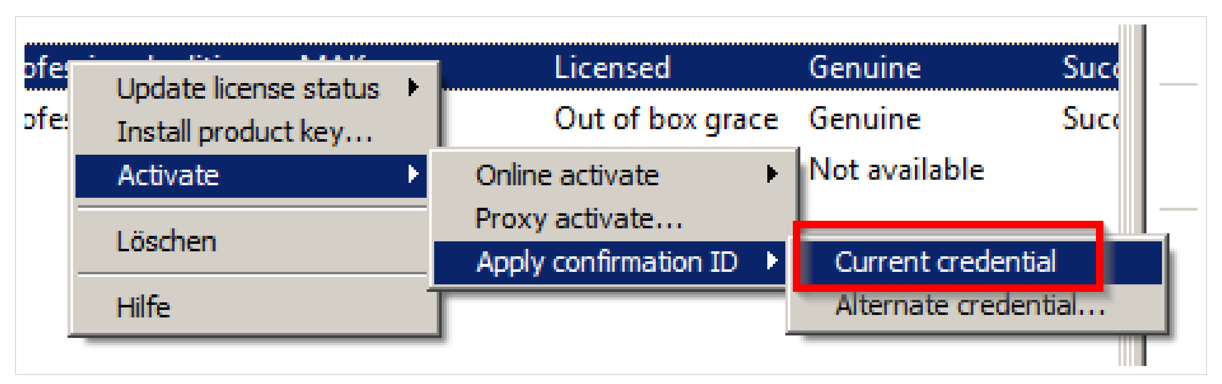


Abb. 238: Zuweisen der bestehenden Lizenz an den Client

14. Updates für die paedML Linux

14.1 paedML Linux Server

Updates für die *paedML Linux* Server werden automatisch über einen zentralen Updateserver im *Support-Netz* bezogen. Dort finden sich Aktualisierungen für die beiden *paedML* Server, die Firewall sowie ein Verzeichnis für *opsi*-Pakete.



Nach erfolgtem Update müssen die Systeme regelmäßig neu gestartet werden.

Melden Sie sich regelmäßig als „*Administrator*“ an der *Schulkonsole* vom Server und vom *opsi*-Server an, um zu überprüfen, ob ein System-Neustart notwendig ist.

„*Benachrichtigungen*“ oben rechts in der Schulkonsole zeigen an, ob ein Neustart notwendig ist.



Abb. 239: Anzeige neuer Benachrichtigungen

Nach einem Klick auf den „*i(nfo)-Knopf*“ wird die Benachrichtigung eingeblendet.



Abb. 240: Meldung , dass das System neu gestartet werden muss

Wenn Sie dem Link „*Modul „Neustarten“* “folgen, gelangen Sie zu einer Schulkonsolen-Maske, über die ein Neustart ausgeführt werden kann.

14.2 pfSense-Firewall

Das Update der Firewall ist im Installationshandbuch beschrieben. Die Firewall sollte regelmäßig auf aktuelle Versionen geprüft und diese sollten ggf. installiert werden.

14.3 Updates/Hotfixes für Windows und opsi-Pakete



Windows-Updates dürfen ausschließlich über die opsi-Pakete „ms-hotfix“ ausgespielt werden.

Manuell auf Rechnern installierte *Windows*-Updates führen zu Problemen.

Standard-Pakete der paedML Linux

Wenn Sie ein frisch installiertes *paedML Linux* System haben, dann befinden sich in Ihrem *opsi*-Depot einige Softwareprodukte, die Sie auf den Arbeitsstationen Ihres Schulnetzwerks ausspielen können.

Hierzu gehören zum Beispiel *Adobe Acrobat Reader*, *Adobe Flashplayer*, *OpenOffice*, *LibreOffice*, *Mozilla Firefox*, *Mozilla Thunderbird*, *Oracle Java*. Zusätzlich werden seitens des *Support-Netzes* Hotfixes für *Windows* oder *Microsoft Office* angeboten[49].

Auf dem *opsi-Server* vorinstallierte opsi-Produkte werden automatisch aktualisiert. Diese Paketaktualisierungen müssen manuell über die *opsi*-Konsole auf die Clients ausgespielt werden.

Um zu überprüfen, ob es Updates für installierte *opsi*-Produkte gibt, müssen Sie in der *opsi*-Oberfläche alle Rechner markieren, die Sie überprüfen wollen. Klicken Sie anschließend auf den Reiter „*Produktkonfiguration*" des Hauptfensters. Sie bekommen installierte Software angezeigt. Sofern es Updates für die Software gibt, wird in der Spalte „*Version*" ein roter Wert angezeigt, der die neue Versionsnummer der Software anzeigt. Bei verschiedenen Softwareständen steht in der Spalte „*Version*" der Eintrag „*mixed*", der ebenfalls rot angezeigt wird.

Um die Software zu aktualisieren, klicken Sie mit der linken Maustaste im Reiter „*Produktkonfiguration*" in das Feld der Spalte „*Angefordert*" des zu aktualisierenden Produktes. Die Auswahl von „*setup*" und die Bestätigung der Änderung führen dazu, dass die Software beim nächsten Systemstart aktualisiert wird.

Produkt-ID	Stand	Report	Angefordert	Version
7zip				
acroread11				
adminvm				
classic-shell				
clientprodukte				
config-win-base	installed	success (setup)		4.0.1-1
dotnetfx				
firefox				
flashplayer				
google-chrome-for-business	installed	success (setup)		37.0.2062.124-2
hwaudit				
italc	installed	success (setup)		2.0.0-3

Abb. 241: Es gibt ein Update für Clientsoftware

Nachträglich installierte opsi-Pakete

Auf dem Server der *SON*-Gruppe werden *opsi*-Pakete für registrierte *paedML* Kunden bereitgestellt. Diese Pakete und Pakete, die von Drittanbietern bezogen werden, müssen manuell im *opsi*-Depot auf dem Backup-Server aktualisiert werden.



Wir empfehlen Ihnen generell das folgende Vorgehen beim Ausspielen von Produktupdates in Ihrem Netzwerk:

1. Installieren Sie Updates auf einem Testclient bevor Sie diese im gesamten Netzwerk verteilen.
2. Wenn alles funktioniert werden die Updates auf allen Clients der Schule ausgerollt.

---

[49] Die Liste der Programmpakete kann mit der Zeit variieren.

3. Aktualisieren Sie anschließend – sofern vorhanden – das lokale Image im Cache der Arbeitsstationen.

14.4Übersicht über Updatezeiten

Es gibt im System verschiedene cron-jobs – das sind zu bestimmten Zeiten wiederkehrende Aufgaben – mit denen verschiedene Elemente der *paedML Linux* aktuell gehalten werden.

Server-Updates	Die Installation von Updates der *paedML* Server wird automatisch ausgeführt. Hierfür gibt es einen cron-job, der freitags um 16:05 Uhr nach neuen Updates sucht und diese gegebenenfalls installiert.
opsi-Produkte	Hierfür gibt es einen cron-job, der täglich um 2:30 Uhr nach neuen opsi-Paketen sucht und diese in das *opsi-depot* auf dem Backup-Server lädt.
Shalla-Liste (Blackliste für Internetzugriff)	Update erfolgt täglich nachts um 1:05 Uhr.

Tabelle 24: Übersicht über Update-Zeiten

15. Steuerung der Internetzugriffe



Bevor im Folgenden das Thema Steuerung des Internetzugriffs erörtert wird, sei die Bemerkung gestattet, dass technische Mechanismen dem Erfindungsreichtum der Schüler vermutlich immer unterlegen sein werden.

Es wird immer wieder Schlupflöcher geben, die Schüler finden, um gesperrte Internetseiten aufzurufen:

- Webproxy-Dienste
- https-Zugriff
- …

Neben technischen Vorkehrungen, die das Surfverhalten kontrollieren sollen, sollten Sie sich pädagogische Ansätze (Ge- und Verbote, Aufklärungsarbeit, …) überlegen und die eigene Frustrationstoleranz erhöhen.

15.1 Definition von Internetregeln

Aufruf über Schulkonsole: Schul-Administration | Internetregeln definieren
Für die Filterung des Internetzugriffs wird ein sogenannter Proxy eingesetzt. Ein Proxy (englisch „proxy representative“ = Stellvertreter, lateinisch „proximus“ = der Nächste) ist der Vermittler zwischen Web-Anfragen aus dem Schulnetz und dem Internet. Diesem Vermittler können verschiedene Aufgaben delegiert werden. Bei der *paedML Linux* kommt der Proxyserver *squid* zum Einsatz.

In der *paedML Linux* überprüft der Proxy beim Aufruf einer Internetseite, ob der Zugriff auf diese Seite erlaubt ist. Ist das nicht der Fall, wird eine Informationsseite angezeigt, die besagt, dass der Aufruf blockiert wurde. Das Werkzeug, das beim Blockieren von Seitenaufrufen zum Einsatz kommt, ist die sogenannte Blacklist, also eine Liste mit Seiten, auf die der Zugriff gesperrt ist. Als Blacklist kommt die *Shalla-Liste*[50] zum Einsatz.

Wenn Sie Ihren Internetzugang mit dem Angebot von *BelWü* kombinieren, dann können Sie zusätzlich den Webfilter von *BelWü* nutzen (vgl. Kapitel 15.4, Seite 228).



Wir empfehlen unseren Kunden grundsätzlich, den Internetzugang mit dem Angebot von *BelWü* zu kombinieren[51]. *BelWü* ist ein erfahrener Dienstleister, der seit vielen Jahren im Bildungssektor aktiv ist.

Neben vielen Vorzügen, wie z.B. der Auslagerung von Diensten wie *Moodle* oder dem Mailserver aus Ihrer Schul-IT, bietet *BelWü* einen regelmäßig aktualisierten Jugendschutzfilter. Dieser Filter kann als *BelWü*-Kunde von Schulen genutzt werden.

Wenn Sie einen anderen Dienstleister nutzen wollen, der Ihnen Zugang über einen

---

[50] http://www.shalla.de/Info/blacklists.html

[51] http://www.belwue.de/produkte.html

Proxyserver bietet, dann können Sie diesen natürlich auch nutzen.

Das folgende Bild zeigt die zwei Standardeinstellungen des Menüs „*Schul-Administration* | *Internetregeln definieren*“:

- „*Kein Internet*“ – wenn diese Regel aktiviert wird, kann keine Seite im Internet aufgerufen werden.
- „*Unbeschränkt*“ – Der Zugriff funktioniert auf alle Internetseiten (außer die durch den Proxy (*Shalla-Liste*/ gegebenenfalls *BelWü*) gefilterten).

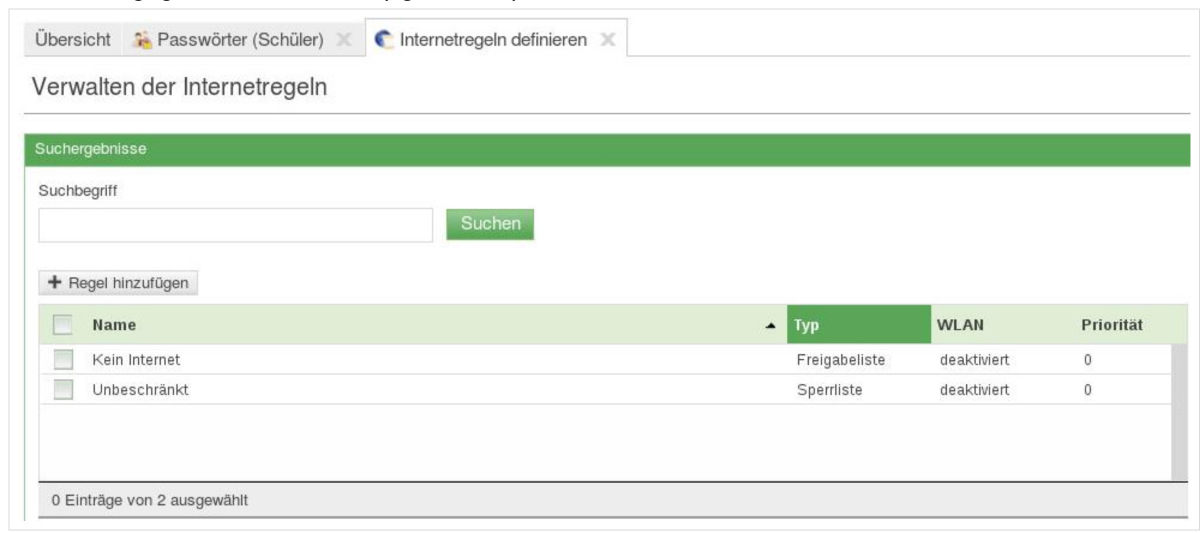


Abb. 242: Standardregeln für den Internetzugriff

Sie können über den Knopf „*Regel hinzufügen*“ eigene Regelwerke definieren. Hierbei gibt es die Möglichkeit, eigene Black- (Sperrliste) und Whitelists (Freigabeliste) anzulegen. Eine Blacklist sperrt bestimmte Seiten, eine Whitelist lässt **nur** den Zugriff auf in der Whitelist eingetragene Seiten zu.

Zuerst ist ein „*Name*“ für die neue Regel einzugeben. Danach wird der „*Regeltyp*“ („*Freigabeliste*“ oder „*Sperrliste*“) definiert.

Im Feld „*Internet-Domänenliste*“ wird festgelegt, welche Seiten aufgerufen werden dürfen oder vom System gesperrt werden. Hier können mehrere Seiten hintereinander eingetragen werden. Es wird empfohlen, den Domänenanteil der Adresse anzugeben, also lmz-bw.de statt www.lmz-bw.de. Tragen Sie jede Domäne in ein eigenes Feld ein.

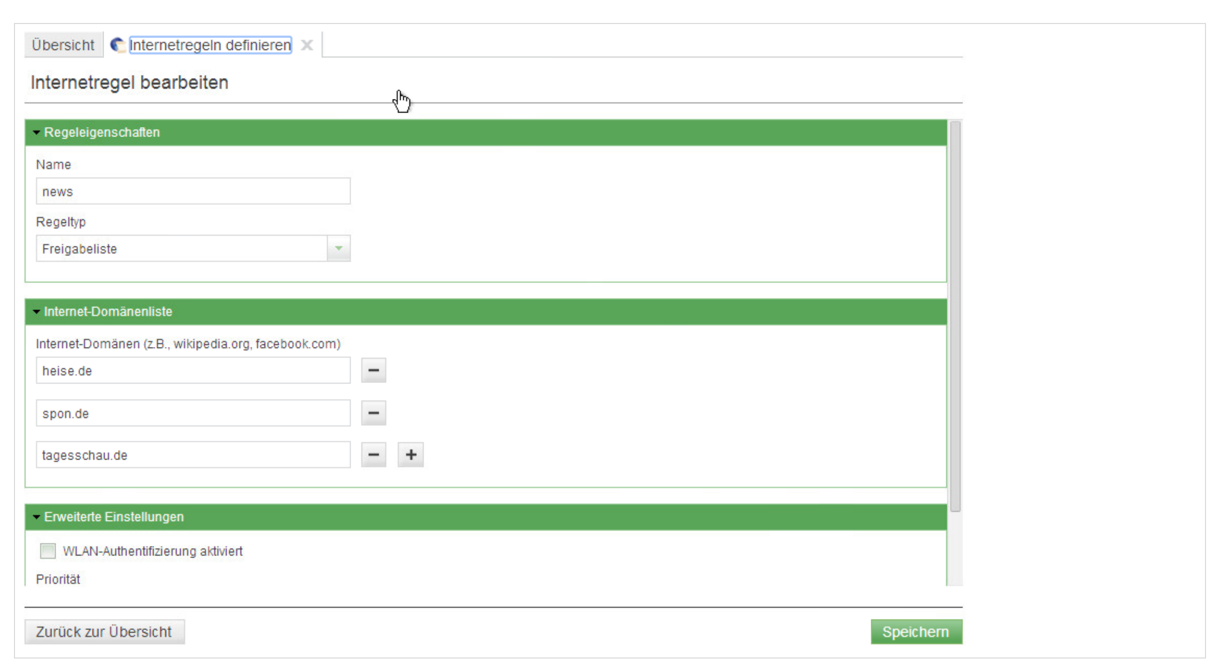


Abb. 243: Anlegen eigener Freigabeliste

Der Haken bei „*WLAN-Authentifizierung aktiviert*" definiert, ob die Gruppe, der die Regel zugewiesen ist, auf ein vorhandenes WLAN zugreifen darf. Wenn der Haken nicht gesetzt ist, Kann sich ein Benutzer nicht am WLAN anmelden, sobald die Regel aktiv ist.

Die „*Priorität*" der Regel legt fest, wie Regeln abgearbeitet werden. Dies ist vor allen dann interessant, wenn Anwender in verschiedenen Gruppen (Klasse und Arbeitsgruppe) Mitglied sind und widersprüchliche Regeln erhalten.

Regeln mit hohen Prioritäten (z.B. 10 (hoch)) überschreiben niedrig priorisierte Regeln (z.B. 0 (niedrig)).

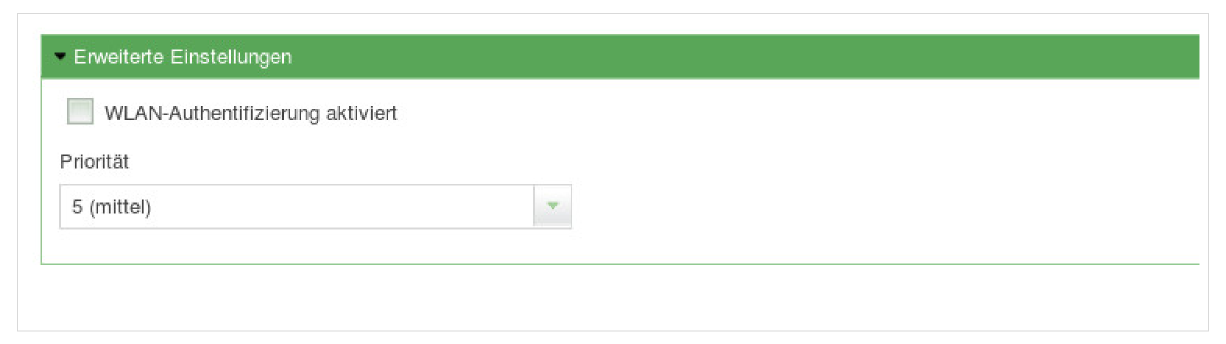


Abb. 244: Anlegen eigener Sperr- oder Freigabelisten

15.2 Internetregeln zuweisen

Aufruf über Schulkonsole: Schul-Administration | Internetregeln zuweisen
Die *paedML Linux* ermöglicht Ihnen die Verwaltung mehrerer Internetregeln, die an verschiedene Benutzergruppen zugewiesen werden können. So können Sie beispielsweise für Unterstufenschüler den Internetzugriff stärker eingrenzen als für Oberstufenschüler.

Die im letzten Abschnitt beschriebene Priorität der Listen entscheidet, welche Inhalte ein Benutzer zu sehen bekommt, wenn er Mitglied verschiedener Gruppen ist.

Die Zuweisung einer Regel erfolgt als Netzwerkberater über das Menü „*Schul-Administration | Internetregeln zuweisen*“. Sie können hier Gruppen auswählen, denen eine bestimmte Regel zugewiesen werden soll. Im folgenden Screenshot wurde das Internet für die fünften Klassen gesperrt. Die sechsten Klassen sollen einen Zugriff auf die Sendung mit der Maus erhalten.

Wählen Sie zunächst die zu ändernden Klassen aus und drücken Sie anschließend auf „*Regeln zuweisen*“. Es öffnet sich ein neues Dialogfenster.



Abb. 245: Zuweisen von Internetregeln an Gruppen

Sie können im nächsten Dialog eine Internetregel an die ausgewählten Gruppen zuweisen. Ein Klick auf „*Regel zuweisen*“ übernimmt die Änderungen.

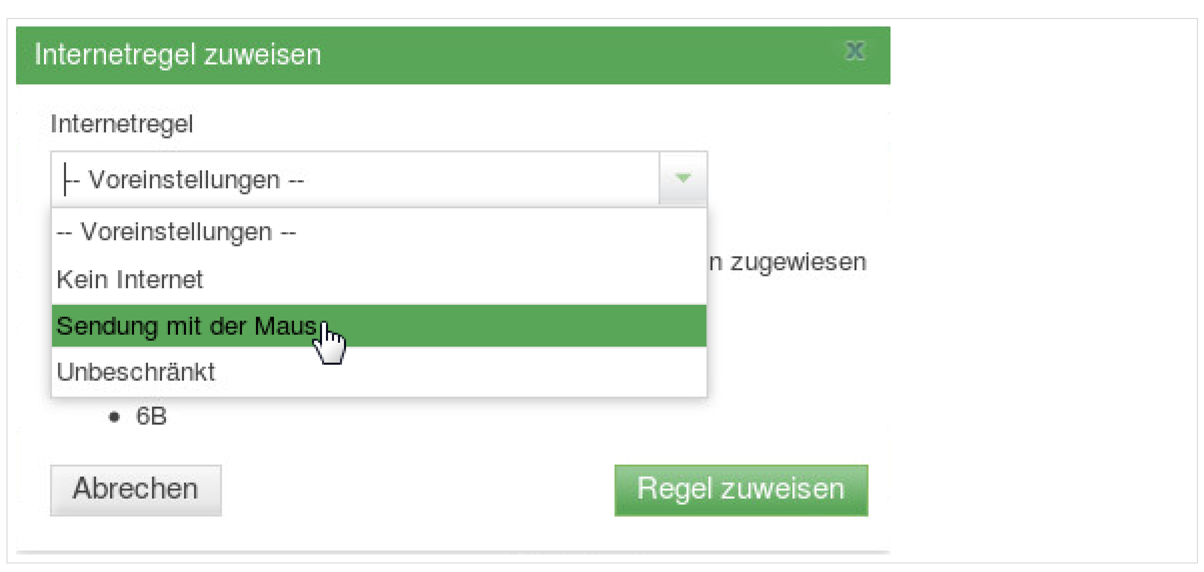


Abb. 246: Auswahl der Internetregel

15.3 Filterung durch internen Proxy

Der Proxy-Server der paedML Linux wird durch die URL-Blacklist „*Shalla´s Blacklists*“ gefiltert. Hierbei werden bestimmte Seiten für den Aufruf gesperrt.

Eine Liste der Kategorien der Shalla Liste kann unter http://www.shallalist.de/categories.html eingesehen werden. Derzeit sind folgende Kategorien aktiv:

adv, hacking, porn, violence, proxy, warez, agressive, drugs, gamble



Die Filterung durch die *Shalla-Liste* und – sofern aktiviert – durch den *BelWü*-Filter ist IMMER aktiv (außer wenn der Jugendschutzfilter komplett deaktiviert wird). Dadurch können bestimmte Seiten nicht aufgerufen werden.



Die *Shalla-Liste* beinhaltet verschiedene Kategorien, die gefiltert werden. Die Liste der Kategorien ist als Unterordner auf dem Server im Verzeichnis /var/lib/ucs-school-webproxy/blacklists hinterlegt. Änderungen der Kategorien können Sie vornehmen, die Hotline kann hierfür aber keinen Support übernehmen. Insbesondere übernehmen wir für die Qualität der Listen keine Gewähr.

Das Ändern der *Shalla-Listen-Einträge* kann **global für alle Rechner des Schulnetzes** über die `UCR-Variable "proxy/filter/blacklists"`[52] vorgenommen werden. Das Hinzufügen oder Entfernen von Verzeichnisnamen des oben genannten Serververzeichnisses bestimmt, welche Kategorien gefiltert werden.

Wenn in der `UCR-Variable "proxy/filter/blacklists"` kein Inhalt steht, ist der Filter deaktiviert. Wir raten jedoch ausdrücklich davon ab, da durch das Deaktivieren der Webfilter im gesamten Schulnetz nicht mehr aktiv ist.

Die in der *paedML* angelegten Filterregeln greifen sowohl auf Rechner im Schulnetz, als auch auf Geräte, die über das Gäste-Netz einen (WLAN)-Zugang haben.

15.4 Eintrag eines externen Proxys

Zusätzlich zum internen Proxy können Sie einen externen Filter aktivieren.

Um einen externen Proxy einzutragen, über den der Netzverkehr des schulischen Netzes gefiltert werden kann, müssen Sie diesen in der *Univention Configuration Registry* (*UCR*) eintragen.

[52] Die Variable kann als Administrator über die Schulkonsole „*System* | *Univention Configuration Registry*“ geändert werden. **Wir raten jedoch dringend davon ab, eigenständige Änderungen in dem Schulkonsolenmodul vorzunehmen, da wir sonst keinen Support für die Installation gewähren können.**

Öffnen sie hierfür das Schulkonsolenmenü „*System* | *Univention Configuration Registry*". Geben Sie in der Suchmaske im oberen Drittel im Feld „*Schlüsselwort*" den Begriff „*squid*" ein. Ein Klick auf „*Suchen*" schränkt die Anzeige der änderbaren Werte ein.

Navigieren Sie zu den Variablen „*squid/parent/host*" und „*squid/parent/port*" und ändern Sie diese nach Ihren Bedürfnissen.

Im Folgenden wurde der Proxy von *BelWü* (Hostname: „*wwwproxy.belwue.de*", Port: „*8080*") hinterlegt.

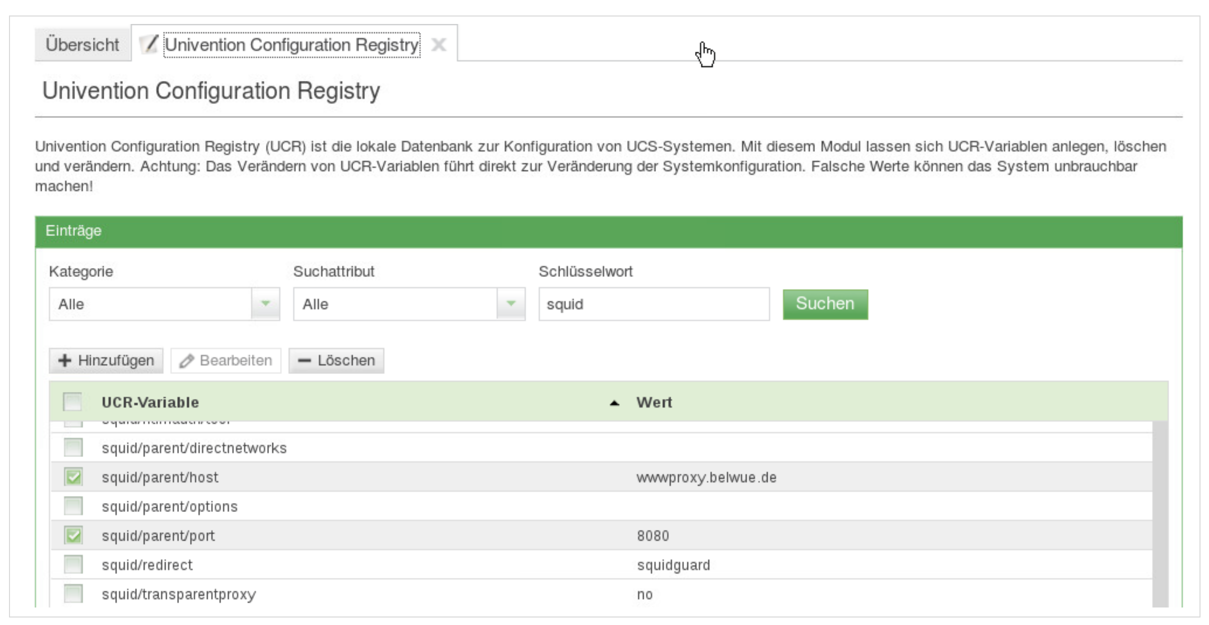


Abb. 247: Eintrag von BelWü-Proxy

Im Anschluss muss der Internetproxy-Dienst „*Squid*" neu gestartet werden.

Der Neustart geschieht über das Schulkonsolenmodul „*System* | *Systemdienste*". Markieren Sie in der Liste der Systemdienste den Dienst „*squid3*".

Im oberen Bereich des Fensters werden nach dem Markieren von Systemdiensten Schaltflächen eingeblendet, über die Sie Dienste starten, stoppen, neu starten,… können.

Drücken Sie auf die Schaltfläche „*Neustarten*".

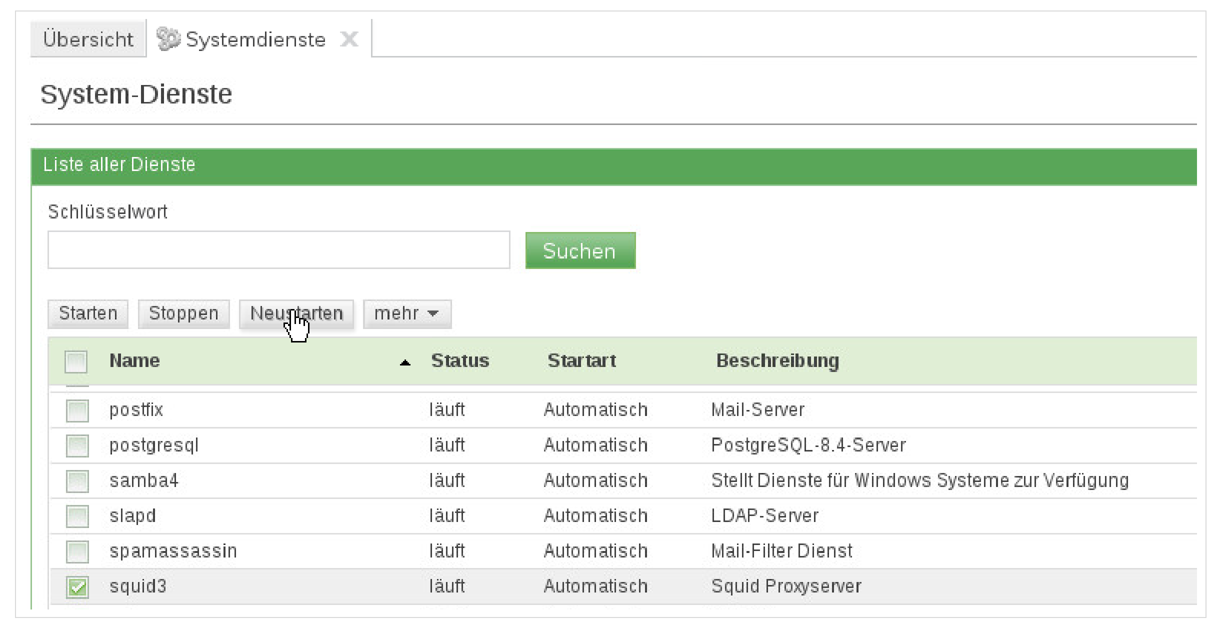


Abb. 248: Nach dem Eintragen eines externen Proxy-Servers ist ein Neustart von Squid notwendig.

Suchabfragen werden nun in der Reihenfolge lokaler Filter, externer Filter abgebarbeitet. Dies heißt, dass zunächst der lokale Filter greift, um eine Anfrage zu blockieren.

GESPERRTE SEITE

Diese Internet-Seite wurde gesperrt. Bitte frage deinen Lehrer um Hilfe.

Abb. 249: Anzeige bei Sperre durch den Webfilter der paedML Linux

Wenn eine Seite nicht vom lokalen Filter, jedoch vom externen Proxy gefiltert wird, blockiert dieser den Zugriff auf den Inhalt der aufgerufenen Seite.



Bitte beachten Sie, dass der externe Filter (sofern aktiv) IMMER greift, auch wenn der interne Filter deaktiviert wurde.

Zugriff verweigert *("content_filter_denied")*



Jugendschutzfilter

Der Zugriff wurde verweigert, da die Seite unter den Jugendschutz oder in eine
andere, von Ihrer Schule/Einrichtung gewünschte Sperrkategorie fällt.

Die Seite wurde in folgende Kategorie(n) eingestuft: "Pornography".

Wenn Sie Zweifel an der Einstufung der Seite haben, so können Sie dies **hier** dem
Hersteller des Filters melden (Filterprdukt: ProxySG)

Weitere Informationen zum BelWü-Webproxy und -Jugendschutzfilter finden Sie **hier**.

Abb. 250: Anzeige bei Sperre durch den Webfilter der paedML Linux

15.5 Sperren von HTTPS-Aufrufen

Ein häufig auftretendes Problem beim Filtern von Internetseiten ist, dass Seiten, die im Webfilter gesperrt wurden, über eine gesicherte Verbindung weiterhin aufgerufen werden können.

Die Ursache hierfür ist, dass der Webfilter auf Port 80, dem Standard-Port des für die Internetkommunikation des Browsers genutzten Hypertext Transfer Protokolls (http), gesetzt wird. Webseiten, die zusätzlich über einen gesicherten HTTPS[53]-Zugang verfügen, bleiben weiterhin verfügbar, da der Seiten-Aufruf über Port 443 geschieht. Auf diesem Port wird nicht gefiltert.

Ein Beispiel:
Der Aufruf der Seite http://www.facebook.com soll unterdrückt werden. Eine Filterregel wird hierfür erstellt. Der Aufruf von https://www.facebook.com ist aber dennoch weiterhin möglich.

Die Lösung für dieses Problem liegt in einer globalen Sperre von https.



Achtung! Wenn Sie die Sperre des HTTPS-Ports durchführen, dann ist kein verschlüsselter Aufruf von Webseiten mehr möglich und die Kommunikation geschieht „im Klartext“ und Informationen werden unverschlüsselt übertragen.

Der Zugriff auf einige Angebote (zum Beispiel Webmail-Dienste mit erzwungener Verschlüsselung, Internetbanking,…) ist damit häufig nicht möglich.

[53] http://de.wikipedia.org/wiki/Hypertext_Transfer_Protocol_Secure

Wenn Sie den Aufruf verschlüsselter Seiten dennoch unterbinden wollen, öffnen Sie in der *Schulkonsole* die „*Univention Configuration Registry*“ (Menüpunkt „*System* | *Univention Configuration Registry*“) Der zu ändernde Registry-Wert ist „squid/webports“. Dieses Feld ist im Auslieferungszustand leer.

Im System wird dabei der Wert auf "80 443 21" gesetzt. Dadurch werden Aufrufe über den Port 80 („Hypertext Transfer Protocol“), über Port 443 (HTTPS („Hypertext Transfer Protocol over SSL/TLS“, welches verschlüsselt ist) und über Port 21 („File Transfer Protocol“) erlaubt.

Setzen Sie die Variable auf den Wert "80", um ausschließlich Port 80, HTTP, oder "80 21", um zusätzlich FTP zu erlauben.

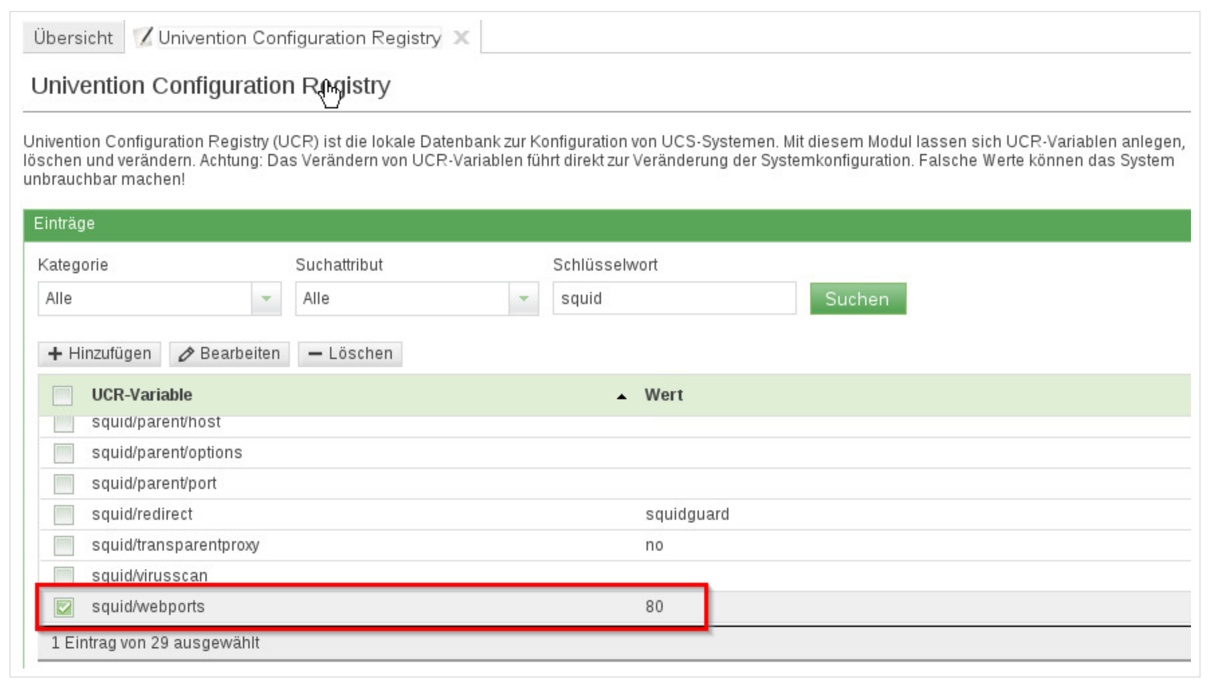


Abb. 251: Einschränken der Netzwerkkommunikation auf Port 80

Im Anschluss muss der Internetproxy-Dienst „*Squid*“ neu gestartet werden.

Der Neustart geschieht über das Schulkonsolenmodul „*System* | *Systemdienste*“. Markieren Sie in der Liste der Systemdienste den Dienst „*squid3*“.

Im oberen Bereich des Fensters werden nach dem Markieren von Systemdiensten Schaltflächen eingeblendet, über die Sie Dienste starten, stoppen, neu starten,… können.

Drücken Sie auf die Schaltfläche „*Neustarten*“.

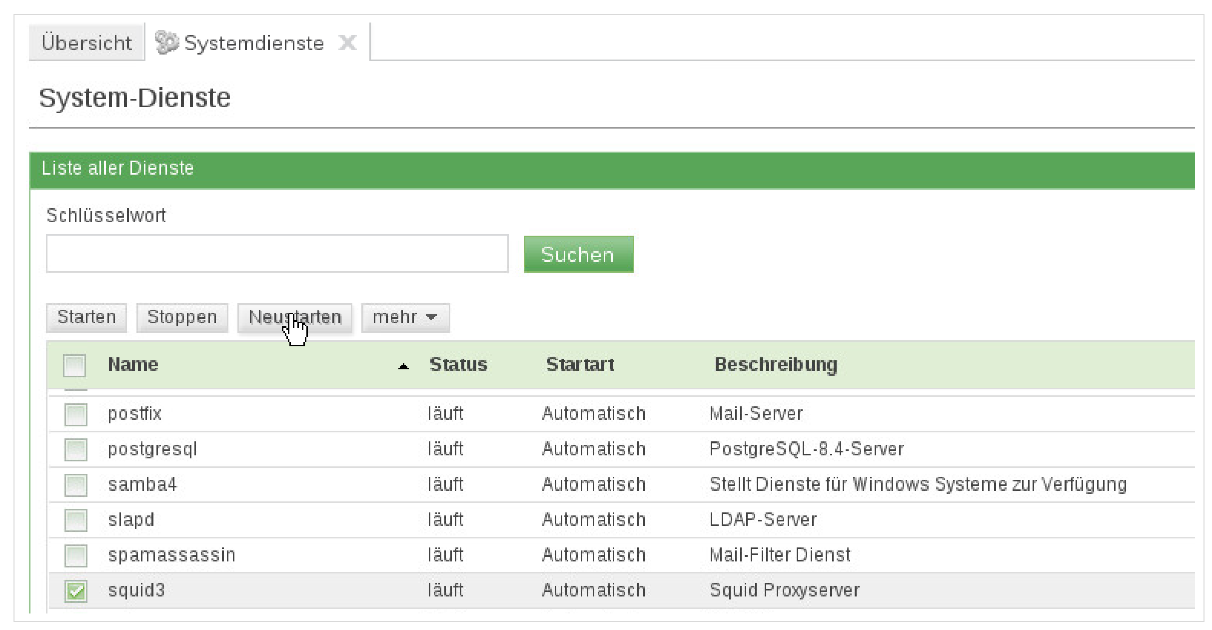


Abb. 252: Nach dem Sperren des HTTPS-Ports ist ein Neustart von Squid notwendig.

15.6 Protokollierung von Internetzugriffen

Leider kommt es immer wieder vor, dass aus dem Schulnetz heraus Missbrauch betrieben wird, der die Ermittlungsbehörden auf den Plan ruft. In einem solchen Fall muss in Erfahrung gebracht werden, welcher Benutzer wann an einem Rechner angemeldet war und welche Seiten er aufgerufen hat.

Die folgende Tabelle listet auf, welches Benutzerverhalten in welchen Dateien protokolliert wird.



Aus datenschutzrechtlichen Gründen ist zur Kontrolle dieser Log-Dateien die Anordnung der Schulleitung einzuholen und das Vier-Augen-Prinzip zu wahren.

Wir empfehlen außerdem, die Benutzer durch eine Benutzerordnung darauf hinzuweisen, dass im Bedarfsfall Log-Dateien ausgewertet werden können.

Protokollgruppe	Verzeichnis	Dateiname	Was wird protokolliert?	Frist
Arbeitssitzung	/home/Administrator/ /home/netzwerkberater	logon.txt	▪ An- und Abmelden von Benutzern an Clients ▪ Datum , Uhrzeit, IP, Benutzername	30 Wochen[54]
	/var/log/	auth.log	▪ System-Log-Datei ▪ Linux-Logins von Diensten (cron,…)	12 Wochen

[54] Bei stark frequentierten Netzwerken können die Dateien weniger als 30 Wochen vorgehalten werden, da ein wöchentlicher Austausch der Log-Dateien stattfindet und zusätzlich ab einer Größe von 50 kB eine neue Log-Datei angelegt wird.

			und root	
Intranet-Webseiten	/var/log/apache2/	access.log	▪ Webseitenname, zugreifende IP, Datum, Uhrzeit	52 Wochen
		other_vhosts_access.log	▪ Webseitenname, zugreifende IP, Datum, Uhrzeit	52 Wochen
Internet-Webseiten	/var/log/squid3/	access.log	▪ Banutzername, Webseitenname, zugreifende IP, Datum, Uhrzeit	2 Tage

Tabelle 25: Log-Dateien zu Benutzerverhalten

Ein Auszug einer Log-Datei zur Veranschaulichung:
Die Informationen zu Seitenaufrufen stehen in der Datei */var/log/squid3/access.log*.

Ein Auszug aus der Log-Datei sieht folgendermaßen aus:

```
(…)

1395996686.010     40 10.1.0.222 TCP_MISS/200 931 GET
http://www.google.com/complete/search? felix.gengler DIRECT/173.194.113.148
text/javascript

1395996686.980    577 10.1.0.222 TCP_MISS/200 25918 GET
http://www.tagesschau.de/ felix.gengler DIRECT/23.74.202.240 text/html

(…)
```

Squid loggt die Zeitstempel in Sekunden seit 1970, so dass eine Umrechnung vorgenommen werden muss, wenn die genaue Zeit ermittelt werden soll. Hierfür gibt es im Internet Angebote, die Sie mit Hilfe der Suchbegriffe „Timestamp & Rechner“ oder „Timestamp & Calculator“ aufrufen können.

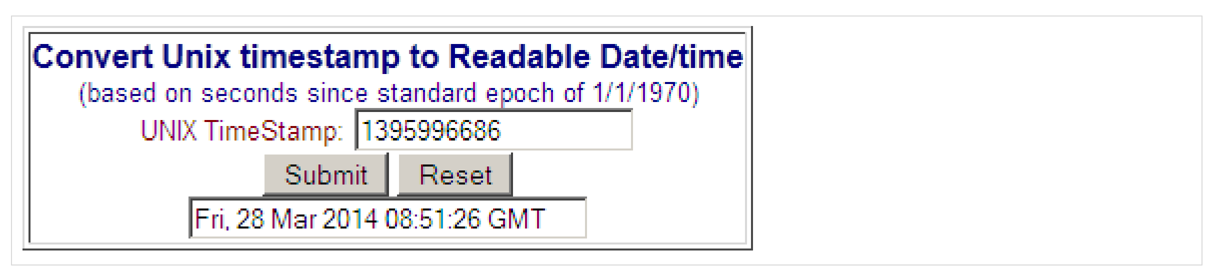


Abb. 253: Umrechnung des Zeitstempels

16. Nagios

16.1 Funktionsweise

Adresse: https://server.paedml-linux.lokal/nagios
Mit der Monitoring-Software *Nagios* werden verschiedene Serverdienste überwacht. *Nagios* ist im Auslieferungszustand so konfiguriert, dass alle drei in der *paedML Linux* eingesetzten Server (Server, Backup und pfSense) überwacht werden.

Im Fehlerfall generiert Nagios eine Mail, die an den Netzwerkberater gesendet wird. Sobald der Fehler behoben wurde, sendet Nagios eine erneute Meldung an den Netzwerkberater.

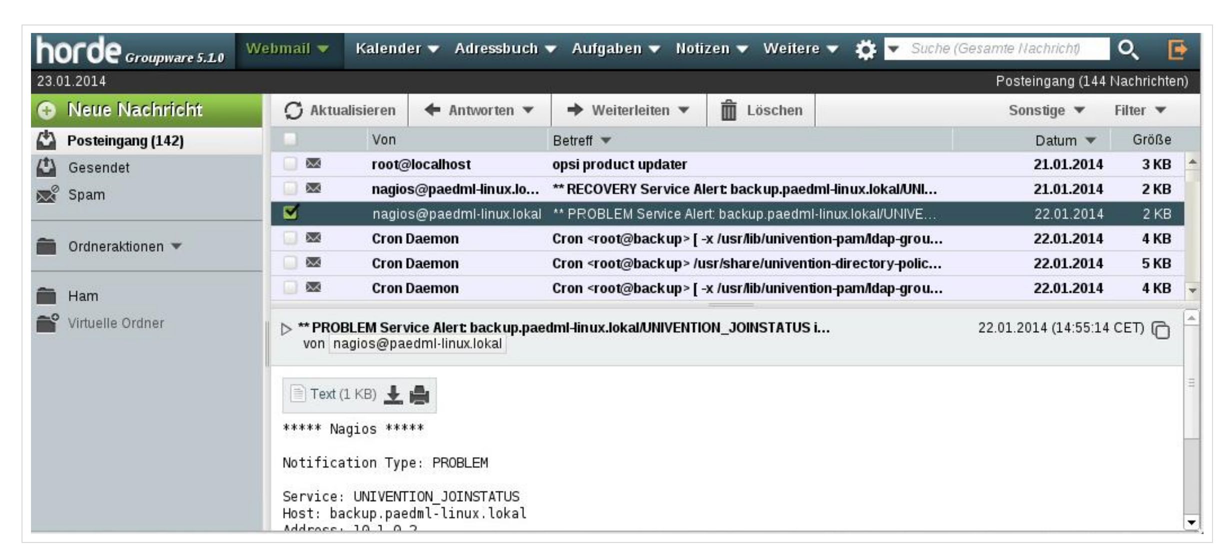


Abb. 254: Nagios-Mail für den Netzwerkberater

Wenn Sie Fehlermeldungen der Standard-*Nagios*-Installation erhalten, nehmen Sie bitte Kontakt mit der Hotline auf. Wenn Sie ein versierter Anwender sind, können Sie Fehler unter Umständen selber beheben.



Hinweis zur Fernüberwachung des Servers mit Nagios:

Die Konfiguration des Nagios-Dienstes in Ihrem paedML Server wird von der Hotline für die Fernüberwachung der Serverdienste genutzt und darf auf keinen Fall geändert werden!

Derzeit steht die Fernüberwachung durch die Hotline nicht zur Verfügung. Wir werden diese Funktion so bald wie möglich nach liefern.



Hinweis für alle anderen Kunden:

Nagios ist als Dienst auf Ihrem Server vorkonfiguriert. Das Programm kann beliebig modifiziert und an Ihre Bedürfnisse angepasst werden. Da es sich um ein mächtiges Programm mit vielfältigen Einstellungsmöglichkeiten handelt, können wir hierfür keinen Support anbieten.

Eigene Anpassungen an der Nagios-Installation werden nicht durch die Hotline unterstützt. Wenn Sie von einem Standardpaket in das Plus-Paket wechseln, sollte der Serverstandard wieder hergestellt werden!

Wir bitten Sie um Verständnis. Danke.

Mehr Informationen zu *Nagios* finden Sie unter http://www.nagios.org/ oder unter http://docs.univention.de/handbuch-3.2.html#nagios::general .

16.2 Die Nagiosübersichtsseiten

Auf der Startseite von *Nagios* wird eine Übersicht über den Zustand der überwachten Maschinen angezeigt.



Abb. 255: Nagios-Startseite

Auf der linken Seite haben Sie eine Navigationsleiste mit verschiedenen Menüs.

Im Menü „*Monitoring*“ können Sie verschiedene Sichten für *Nagios* einsehen. „*Tactical Overview*“ ist der Standard-Startbildschirm von *Nagios*. In dieser Ansicht sehen Sie einen Überblick über alle überwachten Rechner („*Hosts*“), alle überwachten diente („*Services*“), sowie die Einstellungen der Systemüberwachung („*Monitoring Features*“).

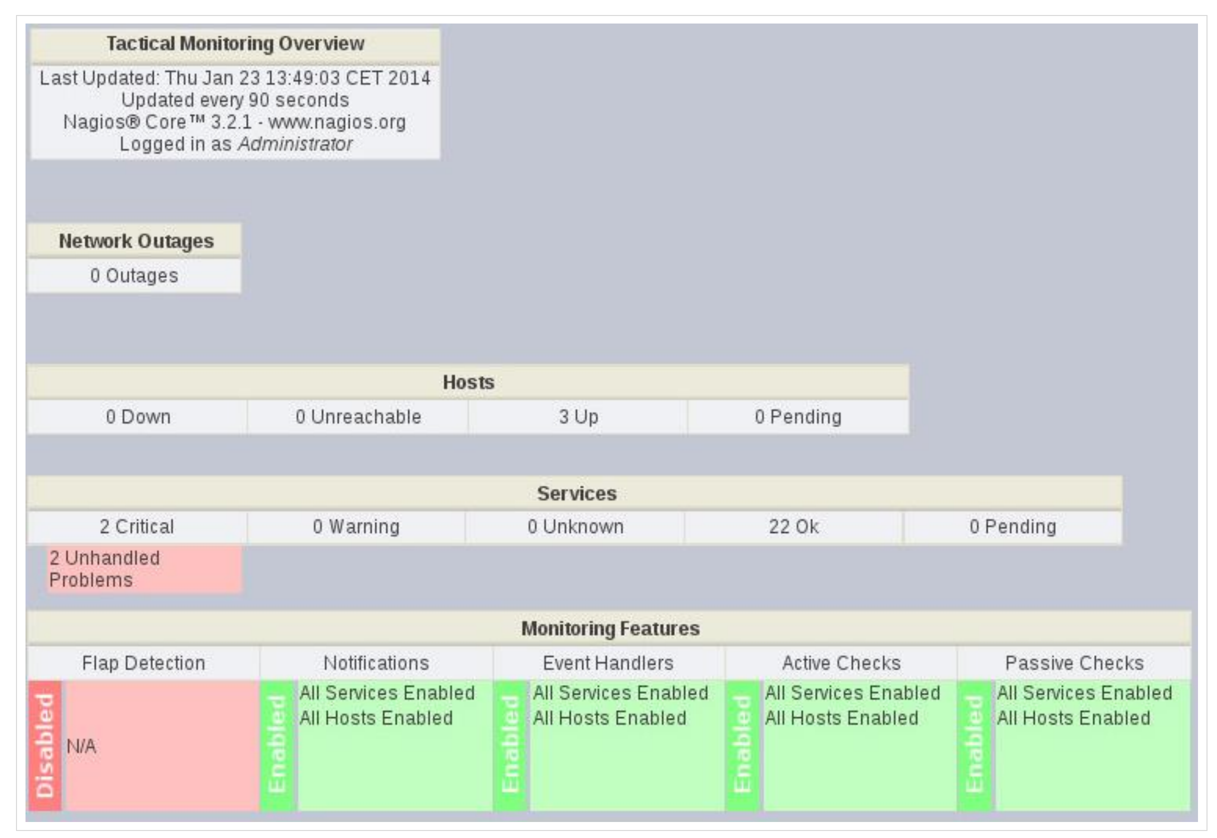
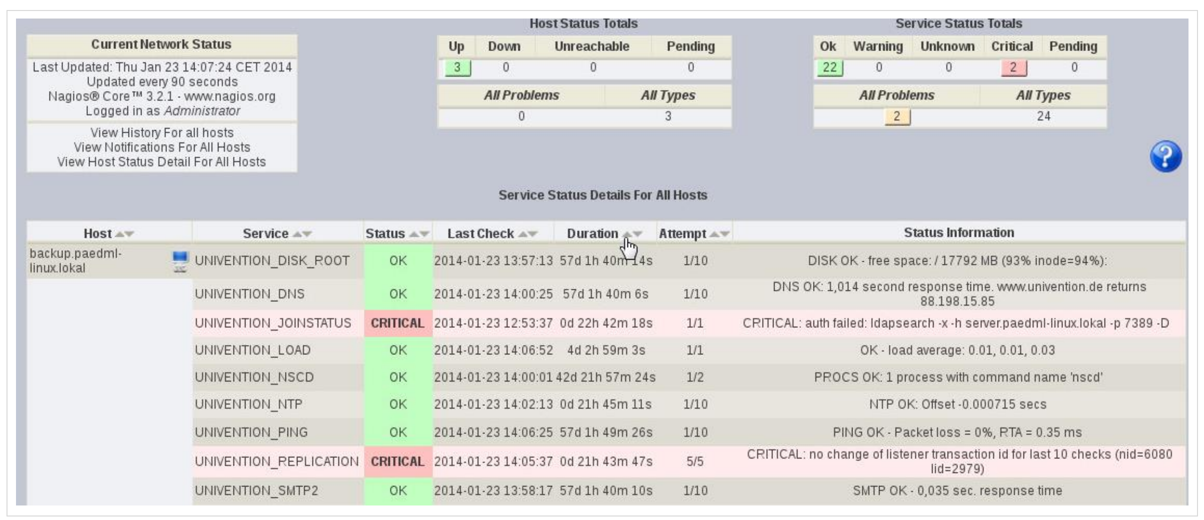


Abb. 256: Die „taktische Übersicht" von Nagios

Unter „*Sevice Detail*" erhalten Sie eine Liste über die einzelnen Dienste (Spalte „*Service*") aller überwachten Maschinen (Spalte „*Host*"). Fehler werden in der Spalte „*Status*" rot unterlegt, im oberen Bereich der Übersicht finden Sie kleine Tabellen, die auf den ersten Blick anzeigen, ob es Probleme gibt und – für den Fall, dass alles in Ordnung ist – das nach unten Scrollen überflüssig machen.



Host	Service	Status	Last Check	Duration	Attempt	Status Information
backup.paedml-linux.lokal	UNIVENTION_DISK_ROOT	OK	2014-01-23 13:57:13	57d 1h 40m 14s	1/10	DISK OK - free space: / 17792 MB (93% inode=94%):
	UNIVENTION_DNS	OK	2014-01-23 14:00:25	57d 1h 40m 6s	1/10	DNS OK: 1,014 second response time. www.univention.de returns 88.198.15.85
	UNIVENTION_JOINSTATUS	CRITICAL	2014-01-23 12:53:37	0d 22h 42m 18s	1/1	CRITICAL: auth failed: ldapsearch -x -h server.paedml-linux.lokal -p 7389 -D
	UNIVENTION_LOAD	OK	2014-01-23 14:06:52	4d 2h 59m 3s	1/1	OK - load average: 0.01, 0.01, 0.03
	UNIVENTION_NSCD	OK	2014-01-23 14:00:01	42d 21h 57m 24s	1/2	PROCS OK: 1 process with command name 'nscd'
	UNIVENTION_NTP	OK	2014-01-23 14:02:13	0d 21h 45m 11s	1/10	NTP OK: Offset -0.000715 secs
	UNIVENTION_PING	OK	2014-01-23 14:06:25	57d 1h 49m 26s	1/10	PING OK - Packet loss = 0%, RTA = 0.35 ms
	UNIVENTION_REPLICATION	CRITICAL	2014-01-23 14:05:37	0d 21h 43m 47s	5/5	CRITICAL: no change of listener transaction id for last 10 checks (nid=6080 lid=2979)
	UNIVENTION_SMTP2	OK	2014-01-23 13:58:17	57d 1h 40m 10s	1/10	SMTP OK - 0,035 sec. response time

Abb. 257: Details zu den überwachten Diensten

Das Menü „*Host Detail*" schließlich zeigt eine Übersicht über alle verfügbaren Maschinen, jedoch ohne die einzelnen Services und deren Status anzuzeigen.

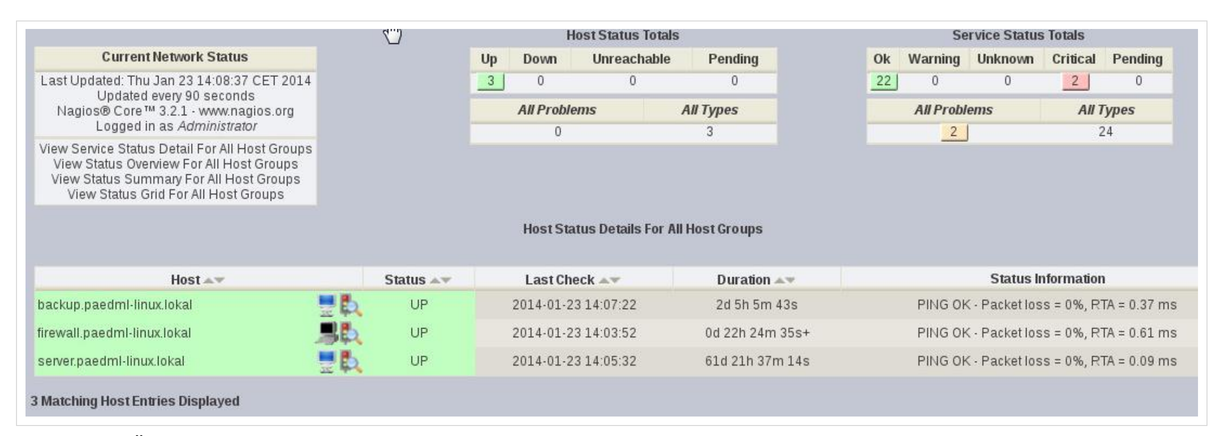


Abb. 258: Übersicht über die überwachten Server

Das Menü „*Reporting*“ bietet Ihnen vielfältige Möglichkeiten über den Status Ihrer Systeme auszuwerten. Sie können sich hier Ansichten erstellen, die beispielsweise zeigen, wie häufig es in einem bestimmen Zeitraum Fehler gab. Dadurch können zum Beispiel regelmäßig auftretende Probleme erkannt und es kann gegengesteuert werden.

Im Menü „*Configuration*“ sollten – wie Eingangs beschrieben – keine Änderungen vorgenommen werden, da Nagios nur im Auslieferungszustand von der Hotline unterstützt wird.



Bei Nagios handelt es sich um ein hochkomplexes Werkzeug zur Überwachung von Computern.

Wenn Sie tiefer in die Materie einsteigen wollen, bitten wir Sie darum die Homepage von Nagios (http://www.nagios.org/) oder einschlägige Internetforen zu besuchen.

Auf der rechten Bildschirmseite sehen Sie eine Übersicht über den Zustand Ihres Netzwerks. Vollständige grüne Balken signalisieren, dass alles in Ordnung ist. Wenn es Probleme gibt, dann werden die Balken kleiner, bzw. rot.



*Abb. 259: Fast alles in Ordnung – die „*Service Health*“könnte noch ein bisschen besser da stehen.*

16.3 Übersicht über die überwachten Dienste

Für das Monitoring bringt *Nagios* eine umfassende Sammlung an Überwachungsmodulen mit. Diese können neben der Abfrage von Systemkennzahlen (z.B. CPU- und Speicherauslastung, freie Festplattenkapazität) auch die Erreichbarkeit und Funktion unterschiedlicher Dienste (z.B. SSH, SMTP, HTTP) testen.

Für die Funktionstests werden in der Regel einfache Programmschritte wie das Ausliefern einer Testmail oder das Auflösen eines DNS-Eintrags durchgeführt. Neben den in *Nagios* enthaltenen Standardmodulen werden auch *paedML*-spezifische Überwachungsmodule mitgeliefert.

Nagios unterscheidet drei grundlegende Betriebszustände für einen Dienst:

„*OK*“ ist der Regelbetrieb

„*CRITICAL*“ beschreibt einen aufgetretenen Fehler, z.B. ein Webserver, der nicht erreichbar ist

„*WARNING*“ deutet auf einen möglicherweise bald auftretenden Fehlerzustand hin und ist somit eine Vorstufe zu „*CRITICAL*“.



Beispiel: Der Test für ausreichend freien Speicherplatz auf der Root-Partition löst erst ab 90 Prozent Füllstand einen Fehler aus, aber bereits ab 75 Prozent eine Warnung.

An diesem Beispiel kann man sehen, das *Nagios*-Meldungen immer im Kontext des jeweiligen Systems gelesen werden müssen. Ein 75%-ige Festplattenbelegung bei einem System mit 200 GB Festplattenspeicher ist kritischer als wenn ein System mit 2 TB Festplattenspeicher zu 75% belegt ist.

Nagios ist also so konfiguriert, dass Dienste überwacht werden, die für die Funktionsfähigkeit der *paedML*-Server benötigt werden. *Nagios* überprüft regelmäßig den Zustand der überwachten Dienste und gibt eine Fehlermeldung aus, wenn es Probleme gibt.

Nagios-Dienst	Funktion
UNIVENTION_PING	Testet die Erreichbarkeit des überwachten UCS-Systems mit dem Kommando ping. In der Standardeinstellung wird der Fehlerzustand erreicht, wenn die Antwortzeit 50ms bzw. 100ms überschreitet oder Paketverluste von 20% bzw. 40% auftreten.
UNIVENTION_DISK_ROOT	Überwacht den Füllstand der root-Partition. Unterschreitet der verbleibende freie Platz in der Standardeinstellung 25% bzw. 10% wird der Fehlerzustand gesetzt.
UNIVENTION_DNS	Testet die Funktion des lokalen DNS-Servers und die Erreichbarkeit der öffentlichen DNS-Server durch die Abfrage des Rechnernamens www.univention.de. Ist für die UCS-Domäne kein DNS-Forwarder definiert, schlägt diese Abfrage fehl. In diesem Fall kann www.univention.de z.B. gegen den FQDN des Domaincontroller Master ersetzt werden, um die Funktion des

	Namensauflösung zu testen.
UNIVENTION_LOAD	Überwacht die Systemlast.
UNIVENTION_LDAP	Überwacht den auf Domänencontrollern laufenden LDAP-Server.
UNIVENTION_NTP	Fragt auf dem überwachten UCS-System die Uhrzeit beim NTP-Dienst ab. Tritt eine Abweichung von mehr als 60 bzw. 120 Sekunden auf, wird der Fehlerzustand erreicht.
UNIVENTION_SMTP	Testet den Mailserver.
UNIVENTION_SSL	Testet die verbleibende Gültigkeitsdauer der UCS-SSL-Zertifikate. Dieses Plugin ist nur für Domänencontroller Master- und Domänencontroller Backup-Systeme geeignet.
UNIVENTION_SWAP	Überwacht die Auslastung der Swap-Partition. Unterschreitet der verbleibende freie Platz den Schwellwert (in der Standardeinstellung 40% bzw. 20%), wird der Fehlerzustand gesetzt.
UNIVENTION_REPLICATION	Überwacht den Status der LDAP-Replikation, erkennt das Vorhandensein einer failed.ldif-Datei sowie den Stillstand der Replikation und warnt vor zu großen Differenzen der Transaktions-IDs.
UNIVENTION_NSCD	Testet die Verfügbarkeit des Name Server Cache Dienstes. Läuft kein NSCD-Prozess wird ein CRITICAL-Event ausgelöst, läuft mehr als ein Prozess ein WARNING-Event.
UNIVENTION_WINBIND	Testet die Verfügbarkeit des Winbind-Dienstes. Läuft kein Prozess, wird ein CRITICAL-Event ausgelöst.
UNIVENTION_SMBD	Testet die Verfügbarkeit des Samba-Dienstes. Läuft kein Prozess, wird ein CRITICAL-Event ausgelöst.
UNIVENTION_NMBD	Testet die Verfügbarkeit des NMBD-Dienstes, der in Samba für den Netbios-Dienst zuständig ist. Läuft kein Prozess, wird ein CRITICAL-Event ausgelöst.
UNIVENTION_JOINSTATUS	Prüft den Join-Status eines Systems. Ist ein System noch nicht Mitglied der Domäne, wird ein CRITICAL-Event ausgelöst, sind nicht-aufgerufene Joinskripte vorhanden, wird ein WARNING-Event zurückgeliefert.
UNIVENTION_KPASSWD	Prüft die Verfügbarkeit des Kerberos-Passwort-Dienstes (nur verfügbar auf Domänencontroller Master/Backup). Läuft weniger oder mehr als ein Prozess, wird ein CRITICAL-Event ausgelöst.
UNIVENTION_CUPS	Überwacht den CUPS-Druckdienst. Läuft kein cupsd-Prozess oder ist die Weboberfläche auf Port 631 ist nicht erreichbar, wird der Status CRITICAL zurückgegeben.
UNIVENTION_DANSGUARDIAN	Überwacht den Webfilter Dansguardian. Läuft kein Dansguardian-Prozess oder ist der Dansguardian-Proxy ist nicht erreichbar, wird der Status CRITICAL zurückgegeben.

UNIVENTION_SQUID	Überwacht den Proxy Squid. Läuft kein Squid-Prozess oder der Squid-Proxy ist nicht erreichbar, wird der Status CRITICAL zurückgegeben.
UNIVENTION_LIBVIRTD_KVM	Prüft den Status eines KVM-Virtualisierungs-Servers über eine Anfrage an virsh und gibt den Status CRITICAL zurück, wenn die Rückmeldung mehr als zehn Sekunden dauert.
UNIVENTION_LIBVIRTD_XEN	Prüft den Status eines Xen-Virtualisierungs-Servers über eine Abfrage an virsh und gibt den Status CRITICAL zurück, wenn die Rückmeldung mehr als zehn Sekunden dauert.
UNIVENTION_UVMMD	Prüft den Status des UCS Virtual Machine Managers über eine Anfrage der verfügbaren Nodes. Können sie nicht aufgelöst werden, wird der Status CRITICAL zurückgegeben.
UNIVENTION_opsi	Überwacht den opsi-Daemon. Läuft kein opsi-Prozess oder die opsi-Weboberfläche ist nicht erreichbar, wird der Status CRITICAL zurückgegeben.

Tabelle 26: Nagios Dienste der paedML Linux

17. Mailserver



Der Einsatz von Mailservern, die von außen erreichbar sind, ist im schulischen Netzwerk nicht unproblematisch:

1. Es gibt rechtliche Rahmenbedingungen, die es zu beachten gilt! (Stichworte: Haftung bei Missbrauch, Datenschutz, …)
2. Es gibt einen nicht unerheblichen organisatorischen Mehraufwand für den Netzwerkberater! (regelmäßige Datensicherung, ständige Verfügbarkeit des Dienstes, …)

Aus den genannten Gründen raten wir vom Betrieb eines schuleigenen Mailservers ab. Hierfür gibt es externe Dienstleister. Wir möchten in diesem Zusammenhang auf das Angebot von www.belwue.de verweisen.

Auf dem *paedML Linux* Server läuft *Horde*. *Horde* ist eine Groupware-Lösung, die neben dem Mailversand auch Kalender und andere Funktionen für die Zusammenarbeit im Team anbietet. Mit diesem Programm kann im Unterricht das Thema E-Mail gelehrt und gelernt werden[55]. Bitte beachten Sie die folgenden Hinweise:

1. **Die Einrichtung von Horde ist NUR für den internen Gebrauch konfiguriert.** Eine Öffnung nach außen ist seitens des *Support-Netzes* nicht vorgesehen und wird nicht durch die Hotline unterstützt.
2. Die Verfügbarkeit der Mailadresse eines Benutzers hängt davon ab, ob der Benutzer beim Anlegen eine Adresse zugewiesen bekommen hat. Benutzer können auch nachträglich über die *Schulkonsole* (Modul: „*Domäne* | *Benutzer*“) eine Mailadresse zugewiesen bekommen.
3. **Der Support seitens der Linux-Hotline beschränkt sich auf den Einsatz von Horde als Mailclient zur Verwendung im Schulnetz. Andere Funktionen – wie das Versenden und der Empfang von Mails außerhalb des Schulnetzes, die Kalenderfunktion oder weitere Features von Horde werden nicht unterstützt.**

Weiterführende Informationen zur Bedienung *Horde* finden Sie unter http://www.horde.org/ .

17.1 Aufruf von Horde

Adresse: https://server.paedml-linux.lokal/horde
Sie können die Webseite von *Horde* von jedem Rechner im Schulnetz über die Adresse https://server.paedml-linux.lokal/horde erreichen. Sofern für den jeweiligen Benutzer ein Mailkonto im System angelegt ist, kann sich dieser mit seinem Kennwort an *Horde* anmelden.

---

[55] Bitte beachten Sie hierfür die Hinweise unter http://lehrerfortbildung-bw.de/sueb/recht/ds_neu/daten/email_unter/ und unter http://www.it.kultus-bw.de/,Lde/830504

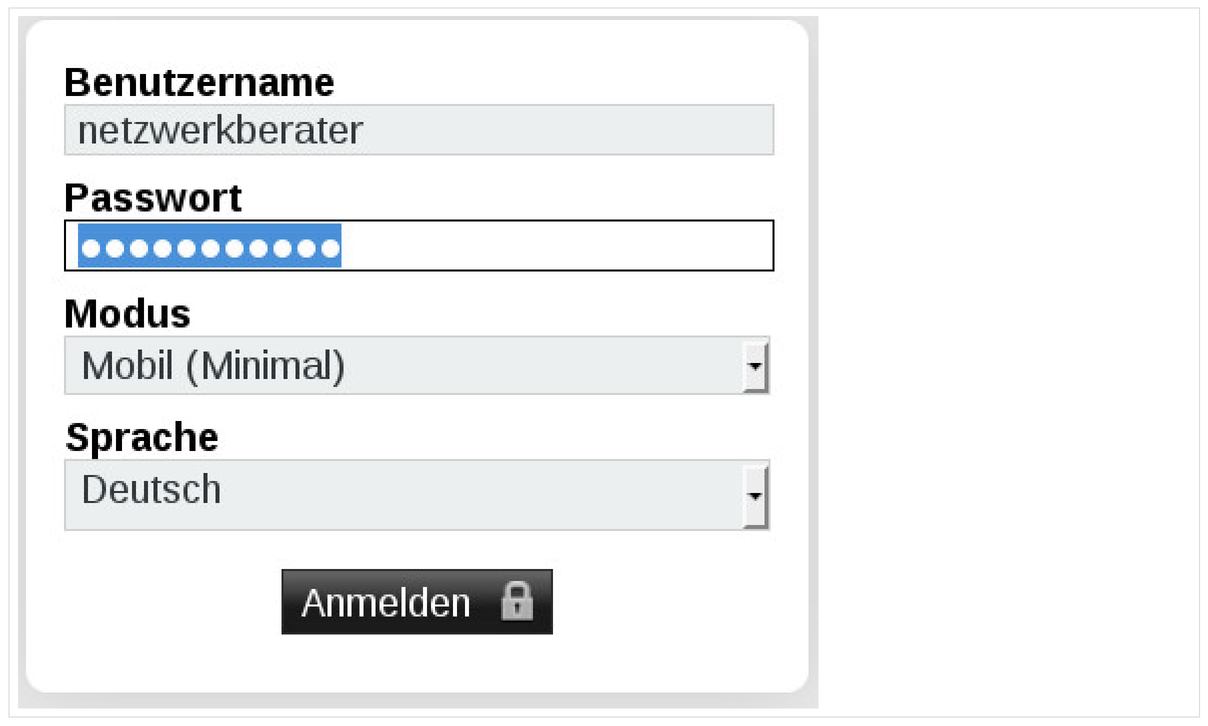


Abb. 260: Anmeldebildschirm von Horde

Nach dem erfolgten Login sehen Sie die Übersichtsseite. Diese gliedert sich grob in zwei Bereiche.

1. Die obere Leiste (1) bietet den Zugriff auf die verschiedenen *Horde* Module. Hier finden Sie Informationen wie das aktuelle Datum und den eingewählten Benutzer. Auf der linken Seite (3) können Sie das Programm konfigurieren oder sich über den orangenen Knopf abmelden.
2. Das Hauptfenster des Programmes (4) zeigt den Inhalt des jeweiligen Moduls an. Im folgenden Screenshot sehen Sie die Übersichtsseite, die Sie nach erfolgtem Login oder durch einen Klick auf das „*Horde*"-Logo oben links aufrufen können. Die Übersichtsseite kann von jedem Benutzer an die eigenen Bedürfnisse angepasst werden. Hierfür klicken Sie bitte auf den Knopf „*Inhalt hinzufügen*" (2).



Abb. 261: Startseite von Horde

17.2 Posteingang

Im vorigen Bild sehen Sie in der Übersicht unter „*Webmail*“ den Status Ihres Posteingangs. Mit einem Klick auf „*Posteingang*“ gelangen Sie in Ihr Postfach.



Abb. 262: Weiter zum eigenen Postfach

Das Postfach gliedert sich in drei Bereiche.

1. Auf der linken Seite (1) sehen Sie die Ordnerstruktur. Hier können Sie zum Beispiel auf gesendete Mails zugreifen.
2. In der Mitte der rechten Seite (3) des Fensters sehen Sie eine Übersicht über Ihre E-Mails.
3. Im unteren Drittel der rechten Seite des Fensters sehen Sie die jeweils ausgewählte Mail angezeigt.

Ein Klick auf „*Neue Nachricht*“ (4) öffnet ein neues Fenster für die Eingabe einer neuen Nachricht.

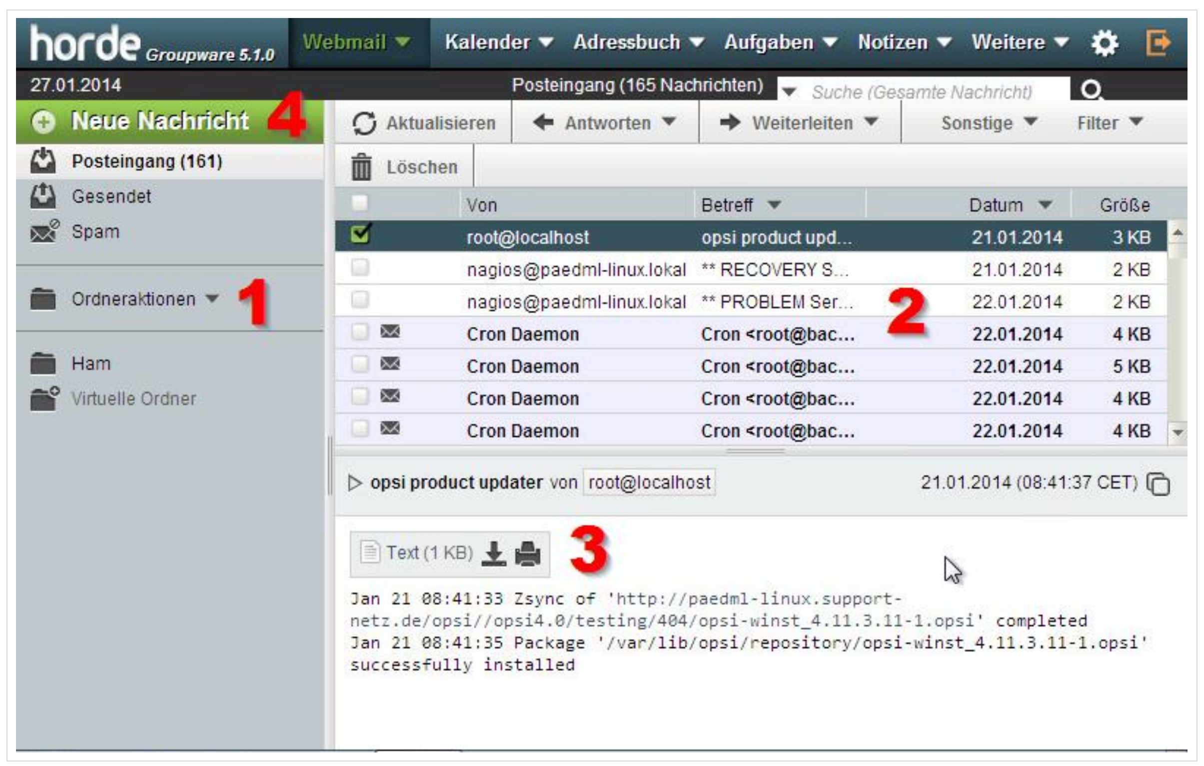


Abb. 263: Der Posteingang

Im Posteingang finden Sie zwei Ordner, die einer kurzen Erläuterung bedürfen:

1. Der erste Ordner „*Spam*“ hilft bei der Einordung von nützlichen und unerwünschten Mails. Der Ordner „*Ham*“ dient dazu Mails, die als „*Spam*“ markiert wurden, aber nicht als solche behandelt

werden sollen, künftig zu erhalten. Hierfür gibt es die Möglichkeit, E-Mails mit einem Bayes-Klassifikator bewerten zu lassen. Dieser vergleicht eine eingehende E-Mail mit statistischen Daten, die er aus bereits verarbeiteten E-Mails gewonnen hat und kann so seine Bewertung an die Mailgewohnheiten anpassen. Die Bayes-Klassifizierung wird vom Benutzer selbst gesteuert, in dem nicht als Spam erkannte E-Mails in den Unterordner Spam verschoben und eine Auswahl legitimer Mails in den Unterordner Ham kopiert werden. Diese Ordner werden täglich ausgewertet und noch nicht erfasste oder bisher falsch klassifizierte Daten in einer gemeinsamen Datenbank erfasst.

   Diese Auswertung ist in der Grundeinstellung aktiviert und kann mit der Univention Configuration Registry-Variable mail/antispam/learndaily konfiguriert werden.

2. Der virtuelle Posteingang („*Virtuelle Ordner*“) ist eine gespeicherte Suchabfrage, die es Ihnen abnimmt, in allen Ordnern nach neuen Nachrichten zu schauen. Stattdessen werden alle Ordner, die Sie für diesen Zweck in der Ordner Navigation ausgewählt haben, automatisch nach neuen Nachrichten durchsucht und in einer einzigen Übersicht angezeigt.

   Diese Funktion ist nützlich, wenn Sie mehrere Mailkonten über Horde abrufen. Da in der paedML Linux nur jeweils ein Mailkonto pro Nutzer aktiv ist; empfehlen wir Mails nur über den Standardordner „*Posteingang*“ zu lesen.

17.3Versand von E-Mails

Es gibt zwei Wege eine neue Mail zu erstellen. Entweder Sie klicken in der Kopfleiste auf „*Webmail | Neue Nachricht*“ oder Sie benutzen den „*Neue Nachricht*“-Knopf im Posteingangsfenster.

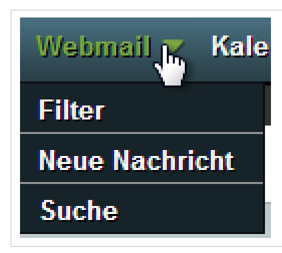


Abb. 264: Detail der Kopfleiste.

Wenn Sie eine neue Nachricht erstellen, dann wird ein neues Browserfenster geöffnet, in dem Sie die Mail bearbeiten können. Für den Versand einer neuen Mail geben Sie den Empfänger (Feld: „*An*“), einen „*Betreff*“ und einen Nachrichtentext ein.

Sie haben verschiedene weitere Optionen wie eine „*Rechtschreibprüfung*“, die Möglichkeit einen „*Anhang hinzu(zu)fügen*“ oder Sie können den „*HTML-Modus*“ aktivieren und die Darstellung Ihrer Mail aufhübschen.

Ein Klick auf „*Senden*“ (oben links) verschickt die erstellte Nachricht.

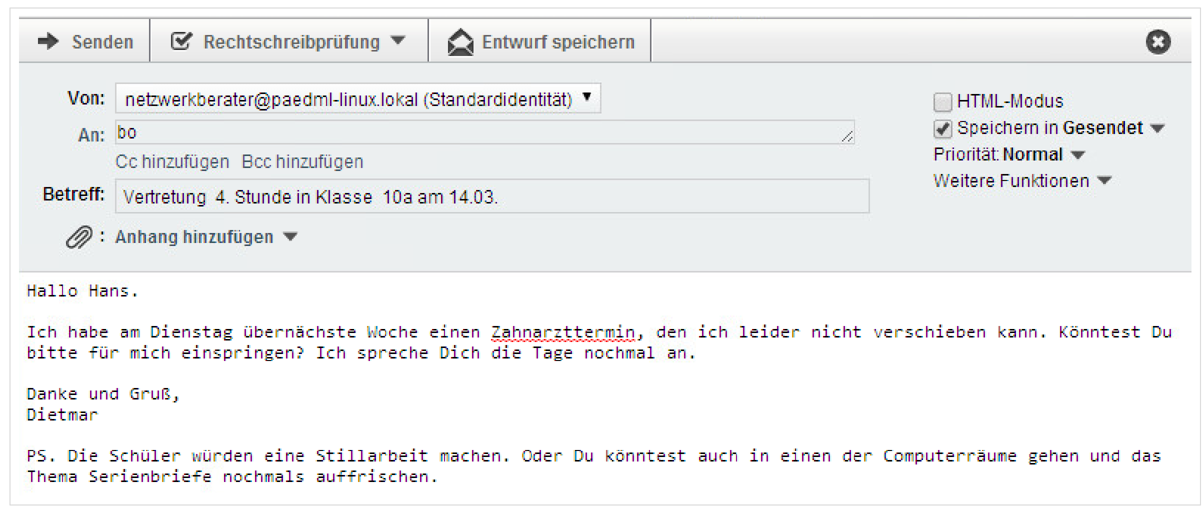


Abb. 265: Fenster für das Erstellen einer neuen Mail

17.4 Änderung von Anhangsgrößen (Attachments)

Die Größen der Anhänge von E-Mails in Horde sind beschränkt auf 10 MB. Eigentlich sollte dieser Wert ausreichend sein, zumal es Tauschverzeichnisse gibt, über die größere Dateien getauscht werden können.

Wenn Sie die Größe der Anhänge in Horde ändern wollen, geschieht dies über die *UCR-Variable: horde/php/apache/cfg/upload_max_filesize*

17.5 Einrichtung IMAP am Beispiel Thunderbird

Anstatt den Webmailer von *Horde* zu nutzen, können Sie auch ein lokales Mailprogramm einrichten und Ihre elektronische Post mit IMAP abrufen. Der Mailempfang via IMAP hat den großen Vorteil, dass alle Mails – bis Sie gelöscht werden – auf dem Server verbleiben.

Gerade als Netzwerkberater ergibt dies Sinn, da ein beliebiges Mailprogramm – am besten das Mailprogramm Ihres Vertrauens – für das Lesen der Systemmails genutzt werden kann. So können Sie zum Beispiel nach Belieben Filter einrichten, die Ihre E-Mails zum Beispiel nach Fehlermeldungen durch Benutzer, *Nagios*-Meldungen,… sortieren.



Abb. 266: Inbox des Netzwerkberaters mit Filterfunktion

Die Konfiguration eines eigenen Mailprogrammes ergibt natürlich nur dann Sinn, wenn der Rechner, von dem Sie die E-Mails des schulischen Netzwerkes bearbeiten wollen, dergestalt konfiguriert ist, dass die Einstellungen dauerhaft sind.



Die Einrichtung des lokalen Mailprogrammes wird hier am Beispiel des aktuellen *Thunderbird* Clients erläutert.

Die notwendigen Schritte zur Einrichtung können zum Zeitpunkt der Einrichtung an Ihrem System abweichen.

Nach der Installation von Thunderbird werden Sie beim ersten Start nach der Einrichtung des Mailkontos gefragt. Dieser Prozess kann auch manuell angestoßen werden, in dem Sie in der Programmübersicht auf „*Neues Konto erstellen*“ klicken.

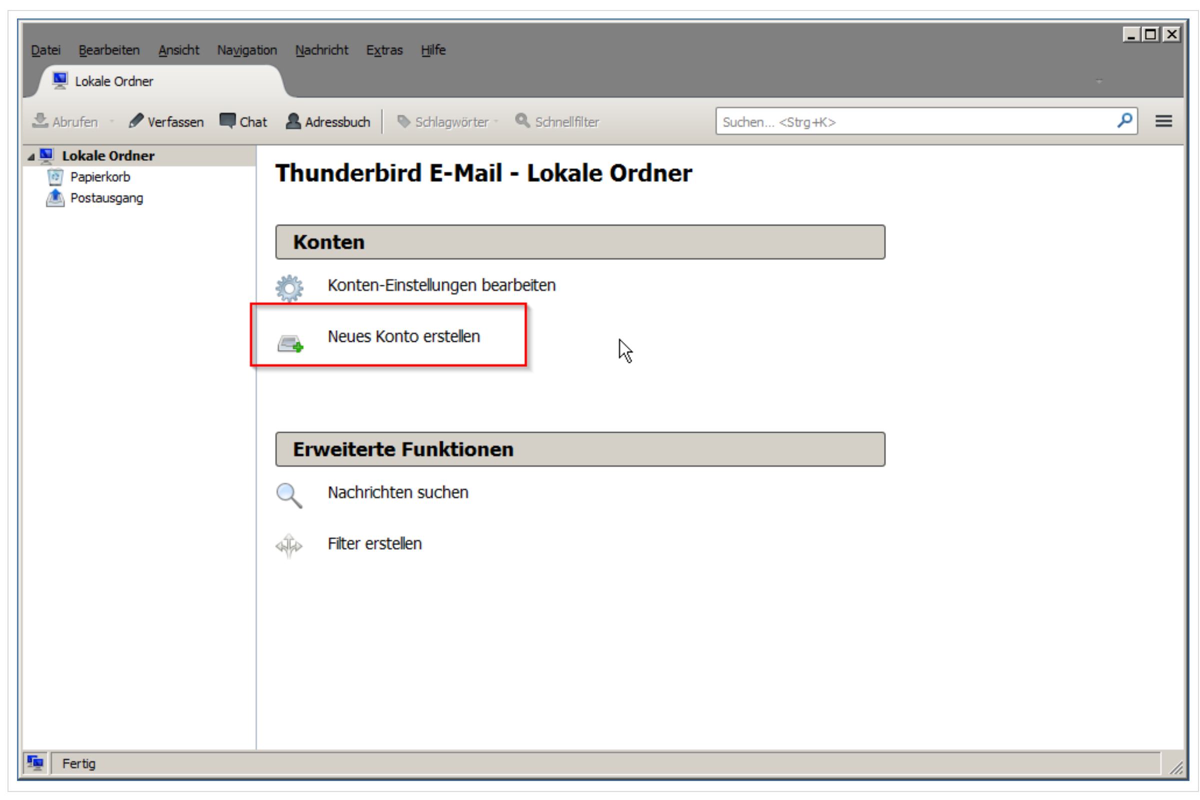


Abb. 267: Erstellen eines neuen Mail-Kontos

Im ersten Feld hinterlegen Sie die Kontoinformationen (beim Versenden angezeigter Name, lokale Mailadresse und Kennwort).

Bitte beachten Sie, dass die Mailadresse im Format „*BENUTZERNAME@paedml-linux.lokal*“ eingetragen wird.

Der Haken bei der Passwortspeicherung ist optional. Wenn Sie das Passwort speichern wollen, so ist dieser Haken zu setzen.

Sie bestätigen die Einstellungen mit „*Weiter*“.

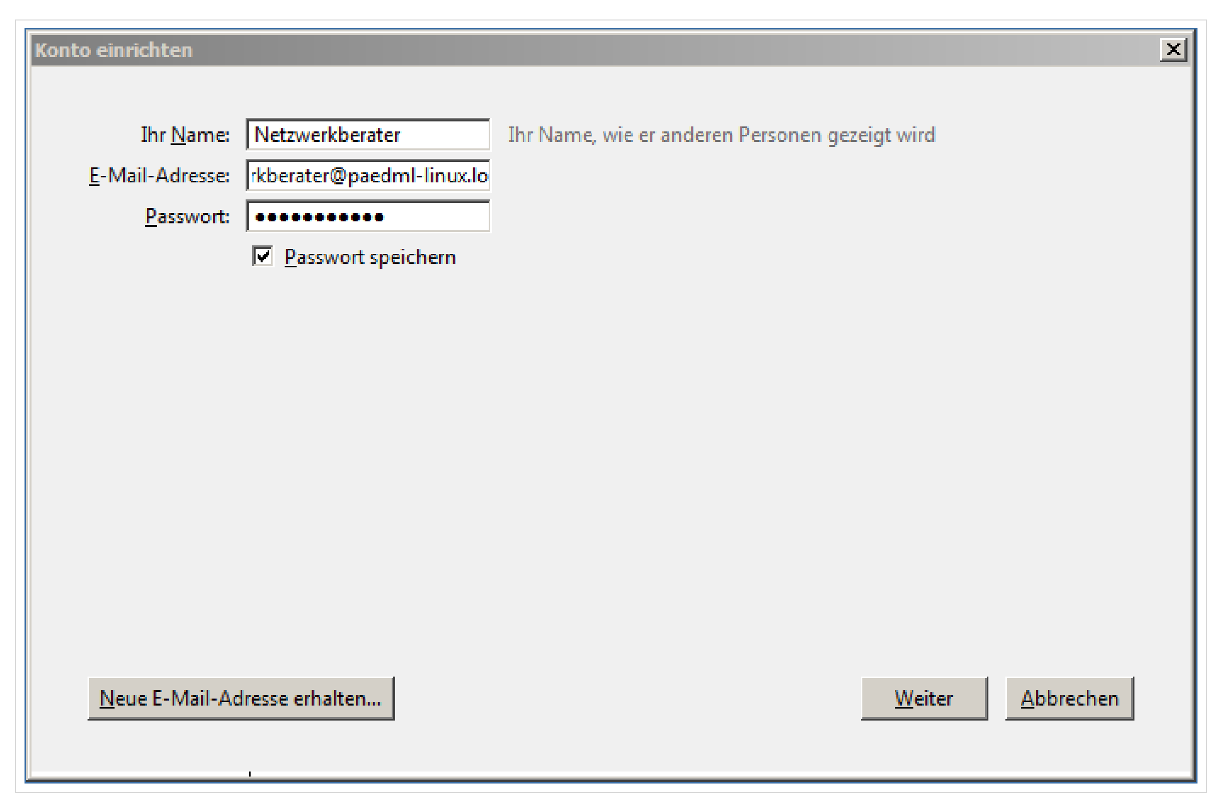


Abb. 268: Eintragen der Benutzerdaten für das Mail-Konto

Anschließend versucht Thunderbird selbständig die Maileinstellungen des Servers zu ermitteln und einzutragen. Dies sollte im Schulnetz funktionieren.

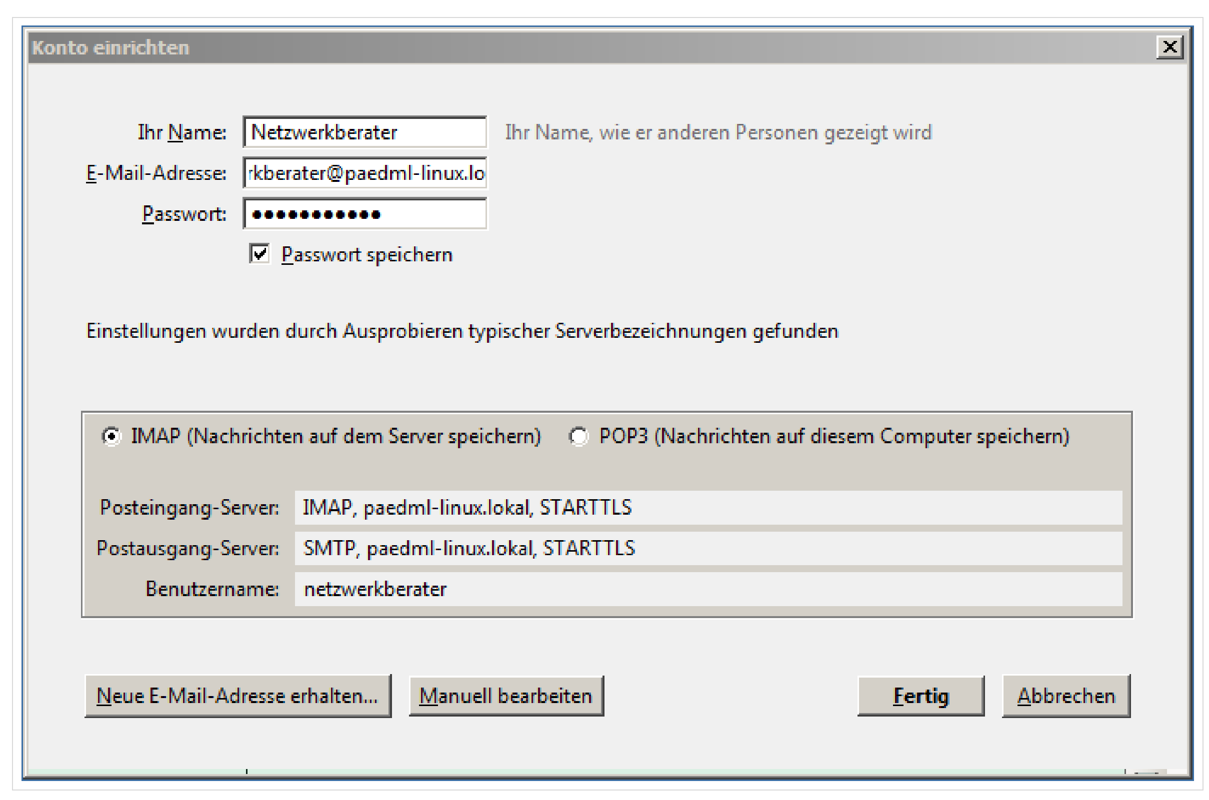


Abb. 269: automatisch ermittelte Einstellungen des Mailservers

Sie können die Einstellungen für das Mailprogramm auch manuell vornehmen:

Posteingangsserver: `server.paedml-linux.lokal`, Port: `143`, Verschlüsselung: `StartTLS`, Authentifizierung: `Passwort, normal`

Postausgangsserver: `server.paedml-linux.lokal`, Port: `25`, Verschlüsselung: `StartTLS`, Authentifizierung: `Passwort, normal`

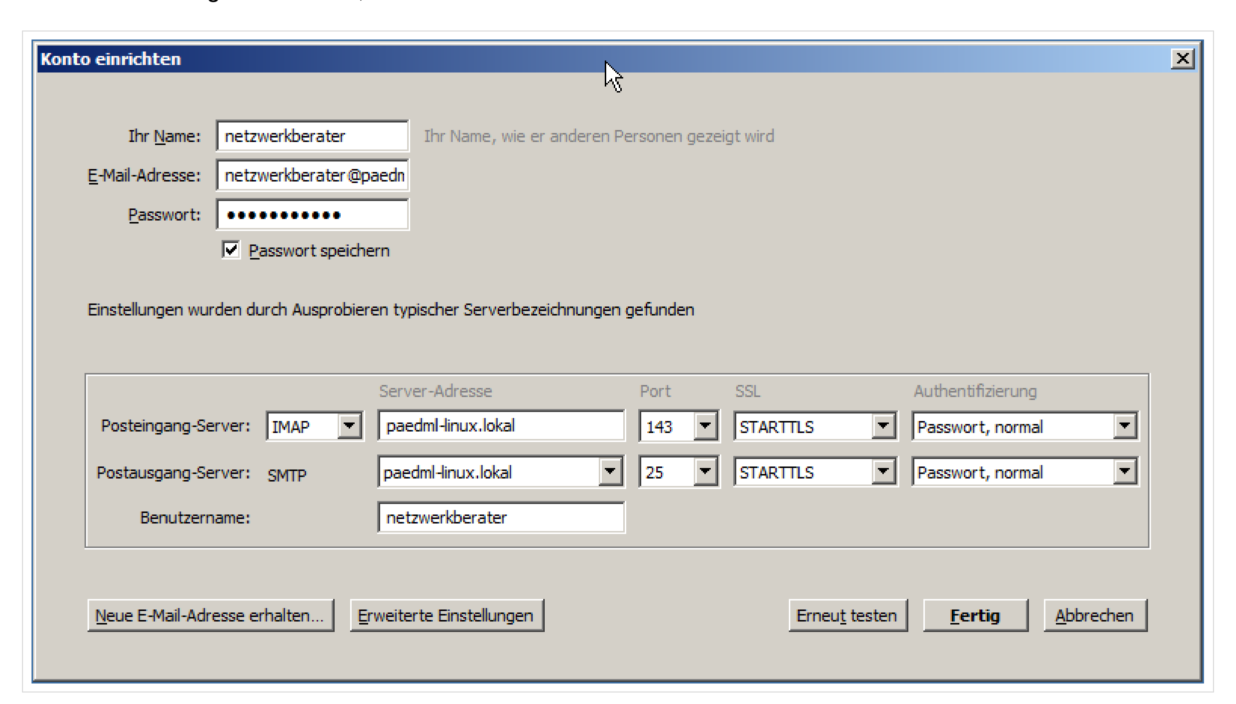


Abb. 270: manuelle Einstellungen des Mailservers

Thunderbird fragt nach der Einrichtung des Kontos beim ersten Verbindungsaufbau, ob dem Serverzertifikat vertraut werden kann. Um die Einrichtung abzuschließen muss das Zertifikat angenommen werden.

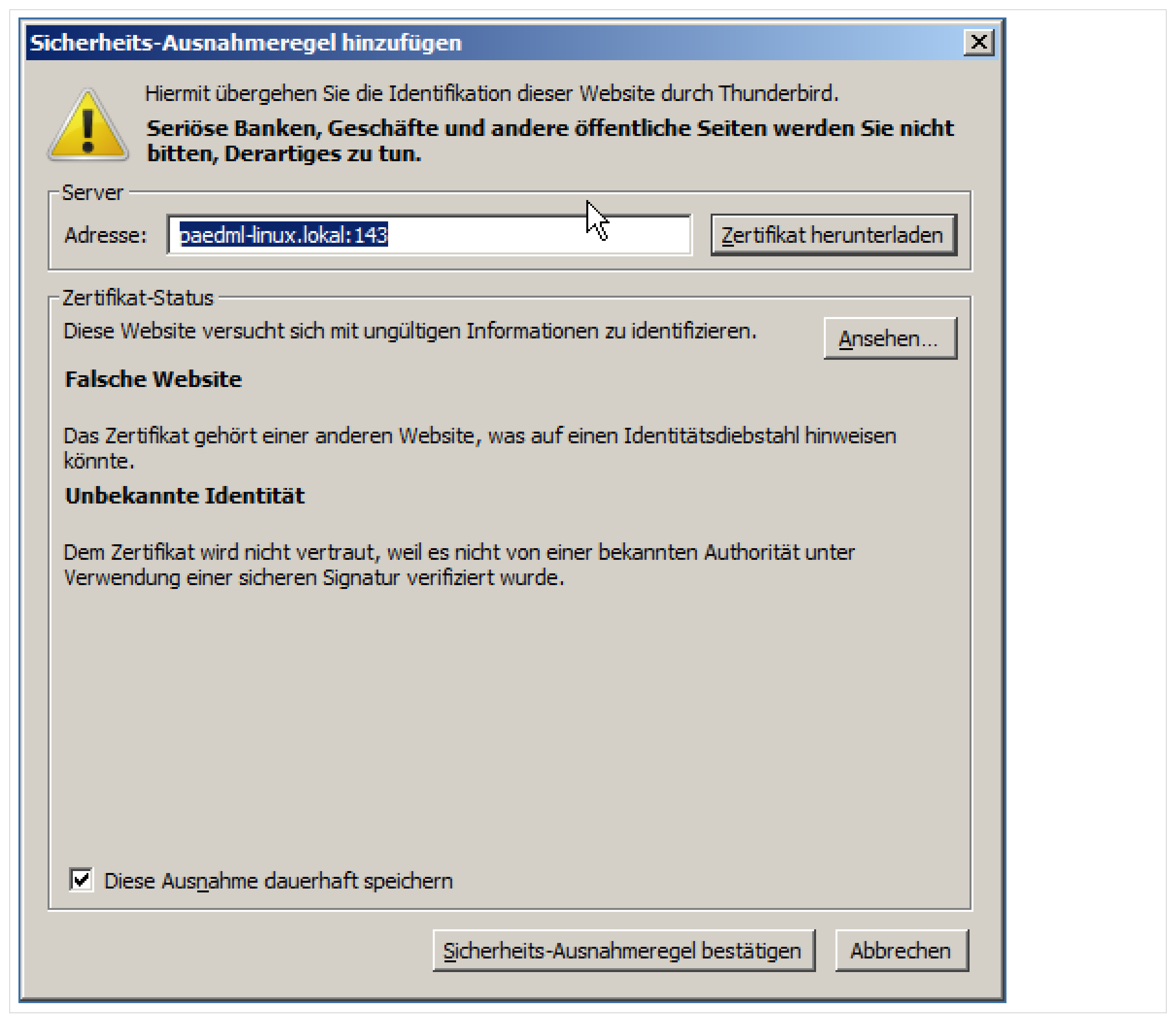


Abb. 271: Abfrage wegen Serverzertifikat.

Nach der erfolgten Einrichtung können Sie E-Mails lokal bearbeiten. Sie können natürlich weiterhin von jedem Rechner im Schulnetz über den *horde*-Webmailer auf Ihre E-Mails zugreifen.

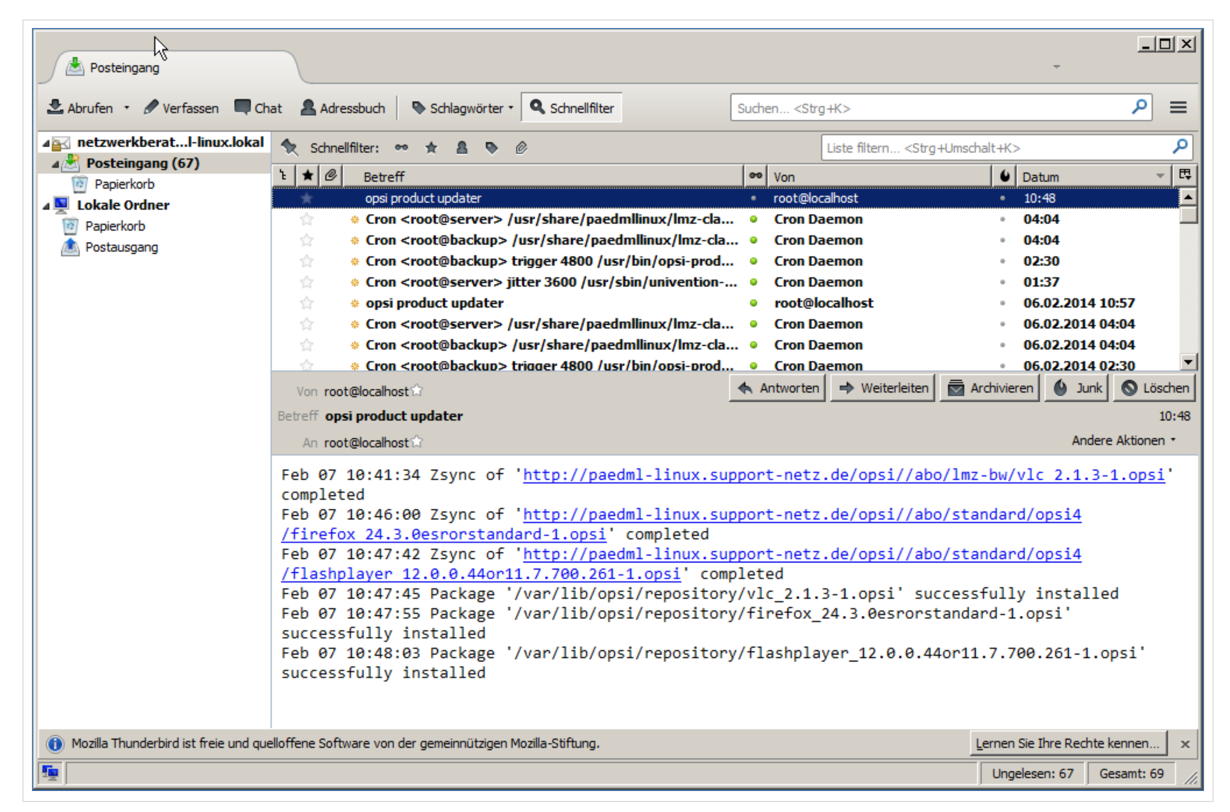


Abb. 272: Erfolgreich eingerichteter Mailclient

18. Helpdesk Modul

Aufruf über Schulkonsole: Unterricht | Helpdesk kontaktieren
Über das Helpdesk-Modul können Lehrer per E-Mail Kontakt zum Netzwerkberater einer Schule aufnehmen. Dadurch können Fehler oder Probleme im Netzwerk an den Netzwerkberater gemeldet werden.

Defekte Geräte, Probleme bei der Ausführung von Programmen, Anwenderfragen oder leere Druckerpatronen. Störungen geben Anlass, Kontakt mit dem Netzwerkbetreuer aufzunehmen. Statt eines Zurufes, oder eines Zettels im Fach, bekommen Sie mit dem Helpdesk Modul eine praktikable Lösung, um Störungsmeldungen im Schulnetz entgegen zu nehmen.

Lehrer können das Helpdesk Modul über das Schulkonsolenmenü „*Unterricht*“ und den dortigen Knopf „*Helpdesk kontaktieren*“ aufrufen.

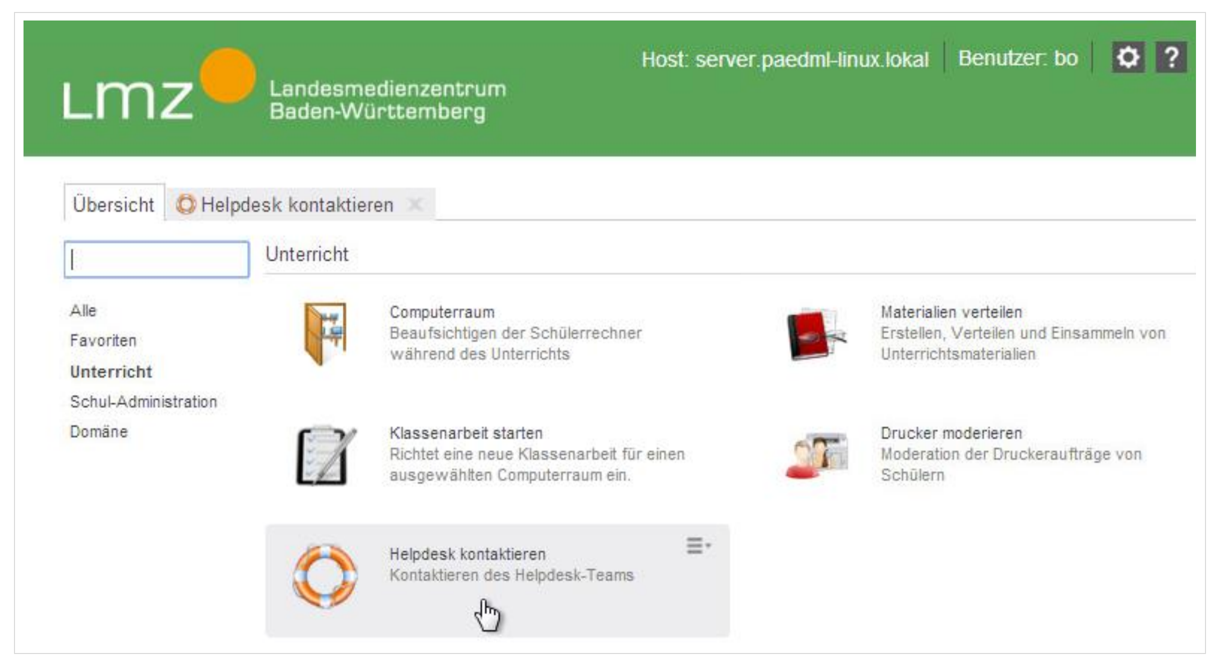


Abb. 273: Aufruf des Helpdesk Moduls

Der „*Benutzername*“ des meldenden Lehrers wird automatisch in die Fehlermeldung übernommen.

Sie können bei der Ticketerstellung zwischen drei Kategorien wählen: “*Hardware*“, „*Software*“ und „*Sonstiges*“.

Nach Auswahl der Kategorie kann im Textfeld „*Nachricht*“ eine Fehlerbeschreibung zur Übermittlung an den *Netzwerkberater* eingegeben werden. Wir empfehlen Ihnen im Kollegium das Modul zu beschreiben und gegebenenfalls die Inhalte der Fehlermeldungen zu spezifizieren.

Schlechte Beispiele für Fehlermeldungen sind:

> *„Im Computerraum funktionieren zwei SchülerPCs nicht mehr!“*
>
> *„Der rote Toner am Farbdrucker ist alle.“*

Qualifiziertere Fehlermeldungen lauten zum Beispiel:

> *„Am Rechner r213-pc01 funktioniert der Monitor nicht."*
>
> *„Die PCs r113-pc07 und r113-pc09 starten nicht. Es gibt die Fehlermeldung „Festplatte nicht gefunden."*
>
> *„Der Farbdrucker in der Kunstsammlung nimmt keine Druckaufträge entgegen. Druckaufträge wurden probehalber von einigen Rechnern im Klassenzimmer aus versendet."*

Die vorangehenden Beispiele setzen voraus, dass die Benutzer die Möglichkeit haben Geräte in Ihrem Netzwerk zu identifizieren. Hierfür raten wir Ihnen die Rechner (zum Beispiel mit Hilfe eines Label-Druckers) mit dem jeweiligen Rechnernamen zu beschriften.

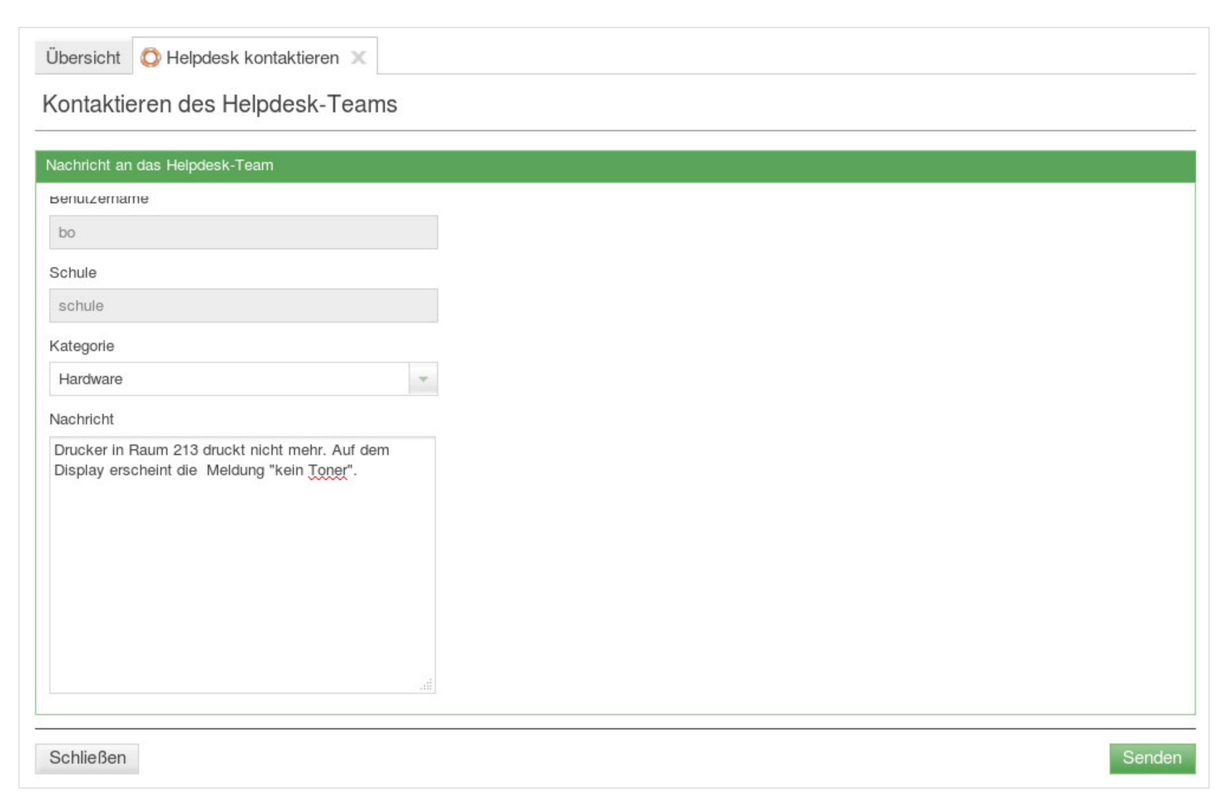


Abb. 274: Verfassen einer Störungsmeldung

Mit dem Mailkonto des Netzwerkberaters können Sie Störungsmeldungen, die über das Helpdeskmodul erstellt worden sind, lesen und bearbeiten. In der Mail enthalten ist der Benutzername, des meldenden Lehrers, das Datum, sowie die Uhrzeit und der Text der Störungsmeldung.

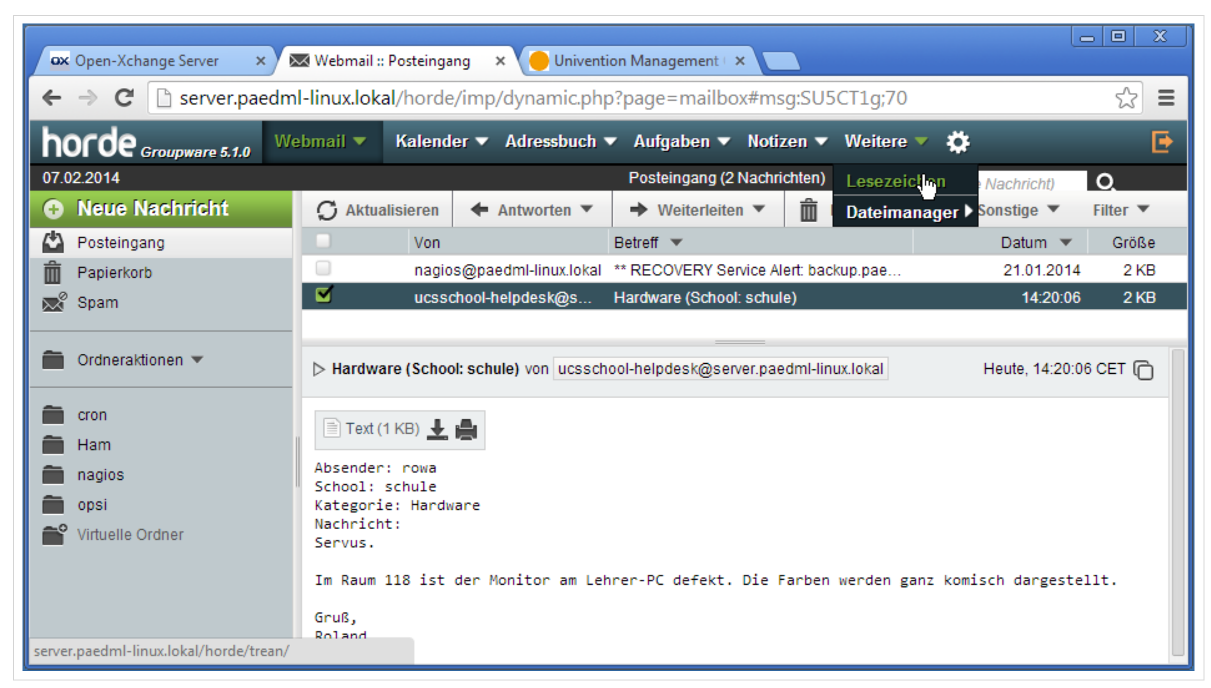


Abb. 275: Mail an den Helpdesk

19. Zugriff von außen via OpenVPN

Der Zugriff von außen, durch Benutzer der *paedML,* wird über *OpenVPN* umgesetzt. Auf das Schulnetz können Lehrkräfte zugreifen. Ein Schülerzugriff ist nicht vorgesehen.

Um auf das Schulnetz von außen zugreifen zu können benötigen Sie

- entweder eine **feste IP-Adresse** für den Internetzugang des Schulservers. Eine solche können Sie bei Ihrem Provider beantragen. So bietet zum Beispiel *BelWü* seinen Kunden feste IP-Adressen, über die das Schulnetz jederzeit erreichbar ist.
- oder einen Dienst, der Ihnen über **Dynamisches DNS**[56] die aktuelle IP-Adresse des schulischen Netzwerkes in einen DNS-Namen übersetzt. Dieses Verfahren ist dann notwendig, wenn Sie **keine feste IP-Adresse** haben, sondern regelmäßig durch Ihren Provider eine neue Adresse zugewiesen bekommen. Beim Dynamischen DNS (auch „*DDNS*") bekommen Sie eine Adresse (zum Beispiel: `meineschule.ddns-beispiel.de`), über die der Zugriff auf die wechselnde IP-Adresse ermöglicht wird. Der DDNS-Server kommuniziert hierfür in regelmäßigen Abständen mit der Firewall Ihres Schulnetzes, um die aktuelle IP-Adresse zu erfragen.

Des Weiteren benötigen Sie das Programm *OpenVPN*[57], mit dem Sie über einen gesicherten Netzwerktunnel von einem externen Rechner auf das *paedML* Netz zugreifen. Die Anbindung geschieht über ein *„virtuelles privates Netzwerk" (VPN)"*[58]. Der verbindende Rechner kann nach erfolgtem Verbindungsaufbau auf Ressourcen im Schulnetz zugreifen.

19.1 Aktivierung von dynamischem DNS in der Firewall



Dieser Abschnitt ist nur zu beachten, wenn Sie keine feste IP-Adresse für Ihr Schulnetz haben. Hierfür müssen Sie sich bei einem Anbieter für einen dynamischen DNS-Dienst registriert haben.

Bitte fragen Sie Ihren Dienstleister bezüglich der Einrichtung von dynamischem DNS und bezüglich der Einrichtung von *OpenVPN*.

Das *Support-Netz* hat im Zusammenhang mit dem Fernzugriff auf die alte *paedML Linux* Hinweise zu DynDNS in einer Anleitung zusammengestellt, die Sie unter http://www.lmz-bw.de/technische-unterstuetzung/kundenportal/linux/erweiterungen/fernzugriff-linux.html abrufen können. Das betreffende Dokument ist die Datei paedML_Linux_Fernzugriff.pdf.

[56] http://de.wikipedia.org/wiki/Dynamisches_DNS

[57] http://openvpn.net/index.php/open-source/downloads.html

[58] http://de.wikipedia.org/wiki/Virtual_Private_Network

Dynamisches DNS wird als Service von Dienstleistern im Internet angeboten. Es gibt kostenfreie und kostenpflichtige Angebote für diesen Dienst. Der Dienstanbieter übersetzt einen DNS-Namen (zum Beispiel „*meineschule.ddns-beispiel.de*") in die jeweils aktuelle IP-Adresse.

Um die Funktion von dynamischem DNS bei einem Anbieter nutzen zu können, muss in festgelegten Abständen ein Signal aus dem Netz mit der dynamischen IP-Adresse gesendet werden, das für die Aktualisierung der IP-Adresse beim Anbieter eines dynamischen DNS-Servers sorgt. Diese Aufgabe übernimmt die Firewall.

Öffnen Sie für die Konfiguration von dynamischem DNS die Übersichtsseite der Firewall (https://firewall.paedml-linux.lokal) und navigieren Sie in den Menüpunkt „*Services* | *Dynamic DNS*". Fügen Sie eine neue Regel hinzu, in der Sie die Einstellungen Ihres DynDNS-Providers hinterlegen. Ein paar Anbieter von dynamischen DNS-Diensten sind schon im System vorkonfiguriert, Sie können aber auch andere Anbieter wählen.

Wenn Sie die Maske zum ersten Mal aufrufen, ist kein DDNS-Service eingetragen. Sie müssen ein neues Profil mit dem im folgenden Bild rot markierten Knopf anlegen.

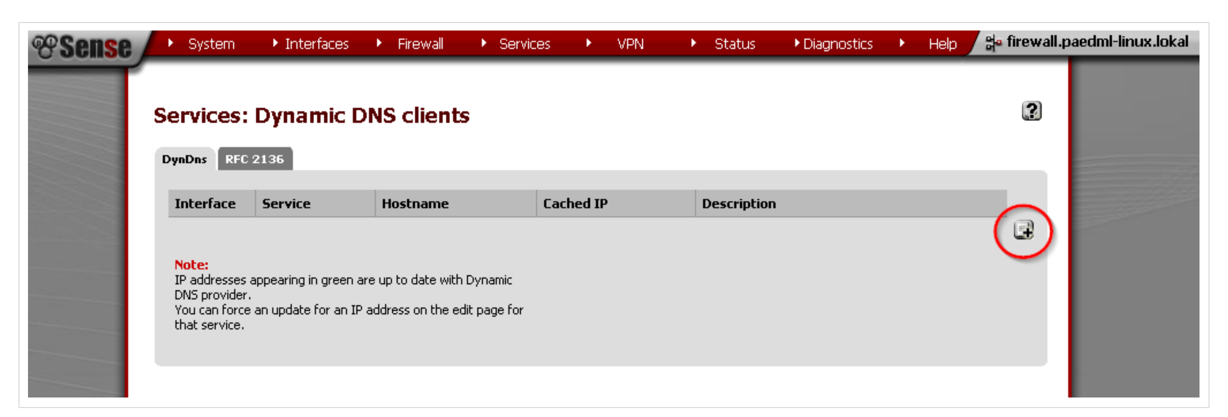


Abb. 276: Noch ist kein DDNS-Dienst eingetragen

Sobald Sie den Knopf gedrückt haben, erscheint eine neue Maske, in die Sie die Zugangsdaten eintragen können.

Entfernen Sie den Haken bei „*Disable*", um den Service zu aktivieren.

Im Dropdownmenü „*Service Type*" sind einige DynDNS-Anbieter hinterlegt. Über die Auswahl von „*Custom*" können eigene Regeln angelegt werden. Dieser Weg wird im Folgenden beschrieben.

Die Dropdown-Menüs „*Interface to monitor*" und (falls vorhanden bei der Anlage einer eigenen „Custom" DDNS-Konfiguration) „*Interface to send update from*" sollten auf den Wert der externen Netzwerkkarte Ihrer Firewall (Standard: „*INTERNET*") eingestellt werden.

Der Haken bei „*Verbose Logging*" aktiviert oder deaktiviert die Ausgabe von Meldungen in die Systemlogdateien der Firewall. Diese Option kann für die Fehleranalyse herangezogen werden (vgl. Kapitel 19.2 auf Seite 258).

Die Werte für die Felder „*Username*", „*Password*" und „*Update URL*" erhalten Sie von Ihrem DDNS-Provider.

Das Feld für „*Result Match*" kann leer gelassen werden.

Im Feld „*Description*“ schließlich können Sie einen Beschreibungstext eingeben, der nach dem Speichern in der Übersichtsmaske unter „*Services* | *Dynamic DNS*“ angezeigt wird.

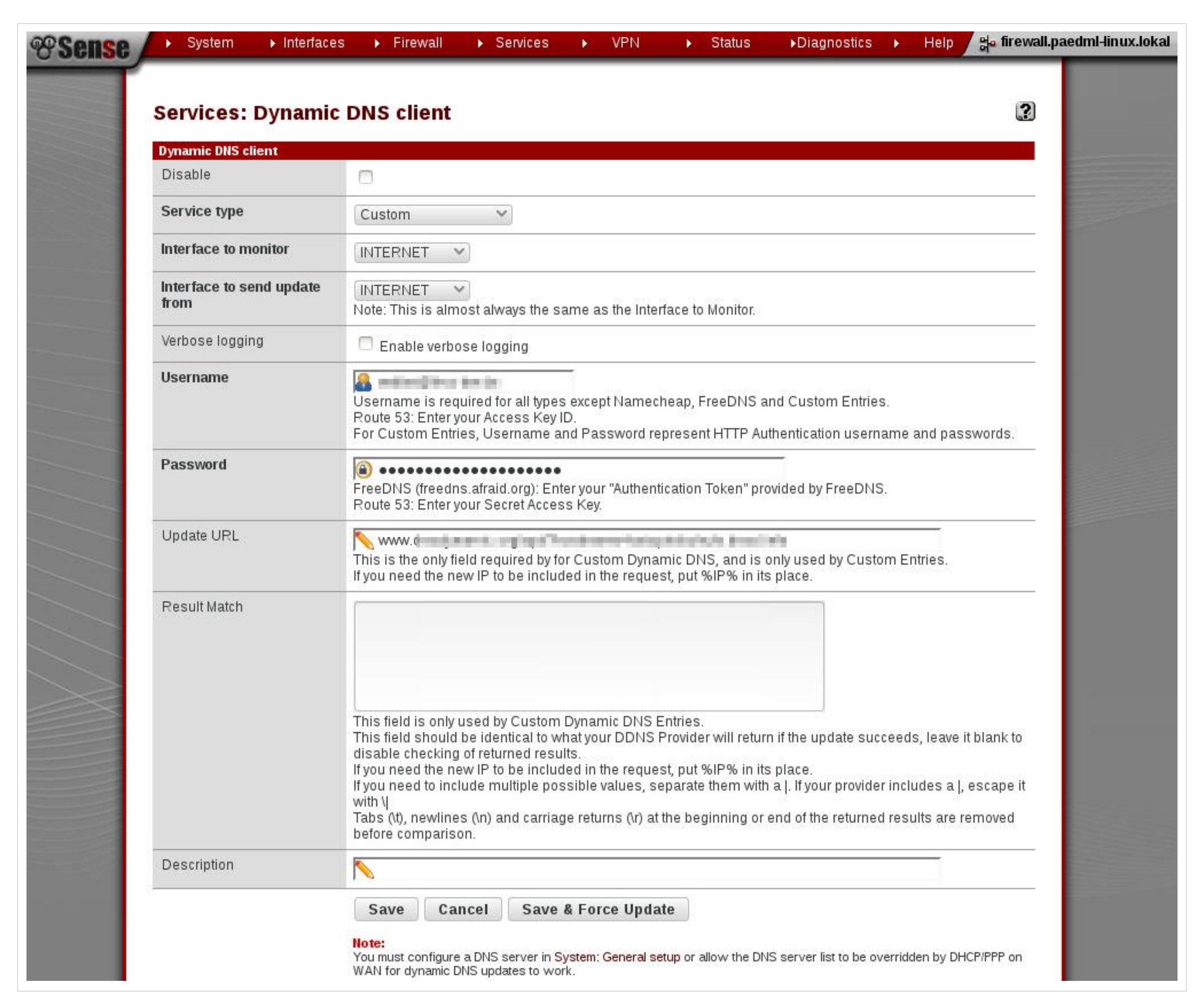


Abb. 277: Dynamisches DNS – Einstellungen in der Firewall

Prinzipiell benötigt DDNS einen funktionierenden DNS-Server im System. Überprüfen Sie über die pfSense-Maske „*System* | *General Setup*“, ob im Feld DNS-Servers gültige Einträge für DNS-Server vorhanden sind.

Das Profil des DDNS-Anbieters wird mit einem Klick auf „*Save*“ gespeichert und in der Übersichtsmaske angezeigt, in der Sie es jederzeit editieren können.

Unterschiede zwischen Custom-Profil und vorkonfigurierten DDNS-Providern

Die in der Firewall bereits hinterlegten DDNS-Anbieter benötigen andere Informationen als ein Custom-Profil. Hier fehlen Eingabefelder, da zum Beispiel keine Adresse für die Aktualisierung der IP-Adresse hinterlegt werden muss. Dafür gibt es zwei neue Felder:

In das Feld „*Hostname*“ wird die Adresse eingetragen, unter der das Netzwerk erreichbar sein soll. Diesen Wert legen Sie bei Ihrem DDNS-Provider an. Zum Beispiel „*meineschule.ddns-beispiel.de*“.

Das Feld „*MX*“ bleibt in der Regel leer. Hier könnte – sofern es der DDNS-Anbieter unterstützt – ein Mailserver erreichbar gemacht werden. **Die Einrichtung eines von außen erreichbaren Mailservers ist nicht Bestandteil der Dienstleistung des Support-Netzes.**

19.2Troubleshooting Einrichtung DDNS-Dienst

Wenn diese neue Regel hinzugefügt wurde, benötigt das System unter Umständen eine Weile, dafür die IP-Adresse zu synchronisieren. Anschließend können Sie versuchen, das Netzwerk von außen zu pingen. Verwenden Sie hierbei den DNS-Namen des Servers. Auf einem Linux-System erhalten Sie die folgende Ausgabe:

```
root@server:~# ping beispielschule.dnsd.info
PING meineschule.ddns-beispiel.de (193.197.xxx.yy) 56(84) bytes of data.
64 bytes from asdf.de (193.197.xxx.yy): icmp_req=1 ttl=64 time=0.273 ms
(…)
--- meineschule.ddns-beispiel.de ping statistics ---
N packets transmitted, N received, 0% packet loss, time 1001ms
rtt min/avg/max/mdev = 0.273/0.280/0.287/0.007 ms
```

Die IP-Adresse 193.197.xxx.yy wurde richtig übersetzt. Das Schulnetz ist über den DNS-Alias meineschule.ddns-beispiel.de im Internet erreichbar. Der Zugriff auf Dienste in diesem Netzwerk (zum Beispiel OpenVPN) muss im Anschluss eingerichtet werden.

Um die Logdateien an der Firewall auszulesen, müssen Sie die virtuelle Maschine der Firewall öffnen und mit der Ziffer `8` die „Shell" (Konsole der pfSense-Firewall) öffnen.

Geben Sie dort den Befehl

```
clog /var/log/system.log | grep -i dns
```

ein. Dieser Befehl sucht in den der Datei „*system.log*" nach Wörten, in denen der Begriff „*dns*" vorkommt. Hieraus kann in der Regel gelesen werden, warum der Dienst nicht funktioniert.

19.3Portweiterleitung für den Zugriff mit OpenVPN

Der DSL-Router muss nun so konfiguriert werden, dass Port 1194 (UDP) an die Firewall weitergeleitet wird. Unter diesem Port läuft der *OpenVPN*-Dienst.

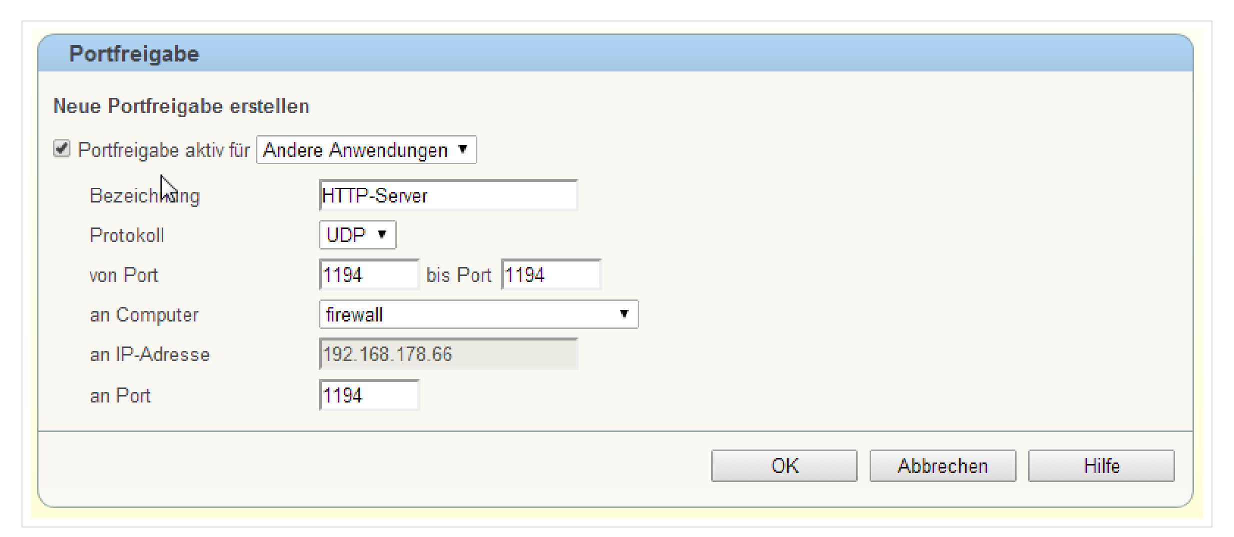


Abb. 278: Freischaltung von Port 1194 an einem Router

In der Firewall gibt es eine vorkonfigurierte Regel, die unter „*Firewall* | *Rules*“ aktiviert ist. Die Regel finden Sie im Reiter „*Internet*“. Bitte überprüfen Sie, ob die Regel aktiviert ist.

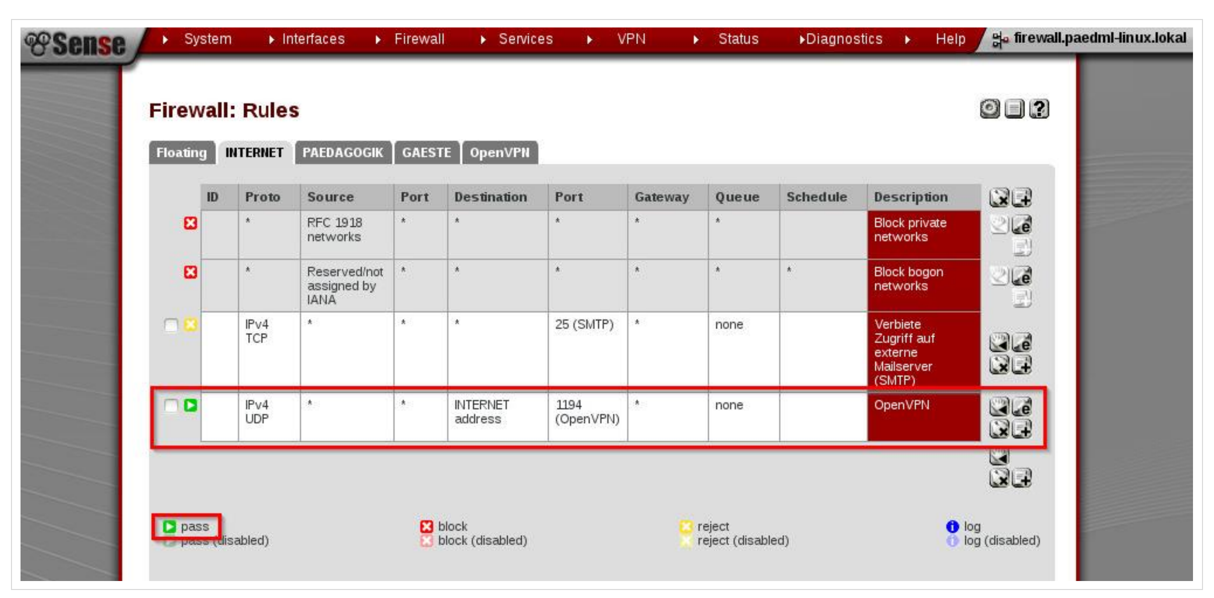


Abb. 279: Die Portweiterleitung für OpenVPN muss ggf. in der Firewall freigeschaltet werden.

Öffnen Sie die Bearbeitungsoption der Regel und überprüfen Sie, ob der Wert „*Action*“ auf „*Pass*“ gestellt ist und kein Haken bei „*Disable this rule*“ gesetzt ist.

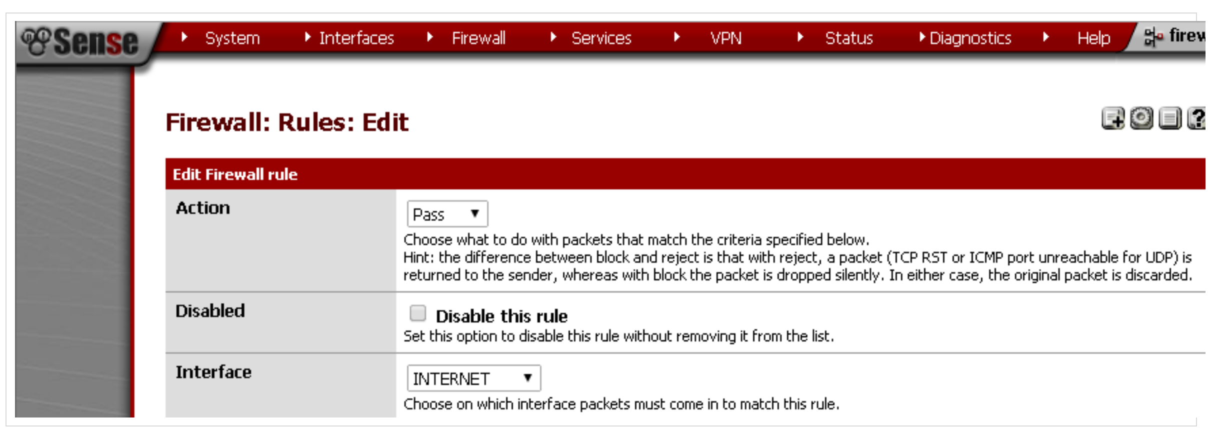


Abb. 280: Überprüfung, ob die Firewallregel aktiviert ist.

19.3.1 Einrichtung von OpenVPN auf dem Client



Wir müssen Sie darauf hinweisen, dass wir nicht gewährleisten können, dass *OpenVPN* auf jedem Rechner funktioniert. Die Einrichtung von *OpenVPN* ist abhängig von Netzwerkparametern (Routerkonfiguration, Firewallregeln,…), Clientbetriebssystem und Version des *OpenVPN*-Programmes.

19.3.2 Wurzelzertifikat des Servers

Um auf den Server von außen zuzugreifen, benötigen Sie das Server-Wurzelzertifikat. Dieses können Sie sich über die Schulkonsole herunterladen und dann auf einem USB-Stick speichern. Um das

Wurzelzertifikat zu erhalten, öffnen Sie die Serverstartseite (https://server.paedml-linux.lokal) und klicken Sei auf „*Wurzelzertifikat*". Mit einem Rechtsklick und der Auswahl von „*Link speichern unter*" können Sie einen Speicherort festlegen.

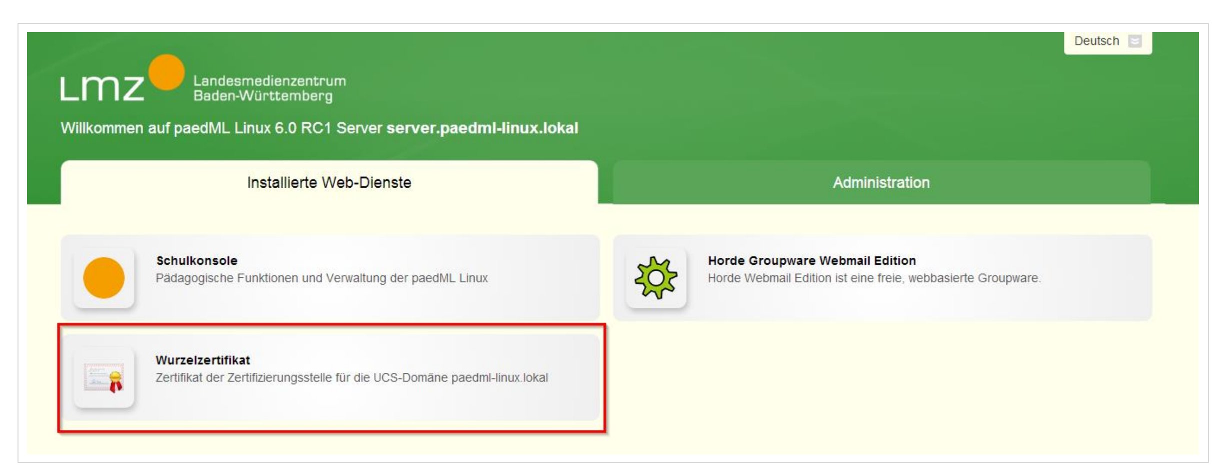


Abb. 281: Hier finden Sie das Wurzelzertifikat

19.3.3 Einrichtung von OpenVPN

Um einen Zugriff von einem externen Gerät in das Schulnetz herzustellen benötigen Sie das Programm *OpenVPN*[59]. Installieren Sie sich das Programm auf dem heimischen PC.

Die Installation von *OpenVPN* benötigt administrative Rechte für den *Windows*rechner. Bei der Installation werden Sie gefragt, ob sie die Gerätesoftware für einen TAP-Netzwerkadapter installieren wollen. Bestätigen Sie diesen Dialog und installieren Sie den Netzwerkadapter. **Achtung! Da diese Software nicht von Microsoft signiert wurde, kann es sein, dass sich OpenVPN nicht unter Windows 8.1 installieren lässt!**

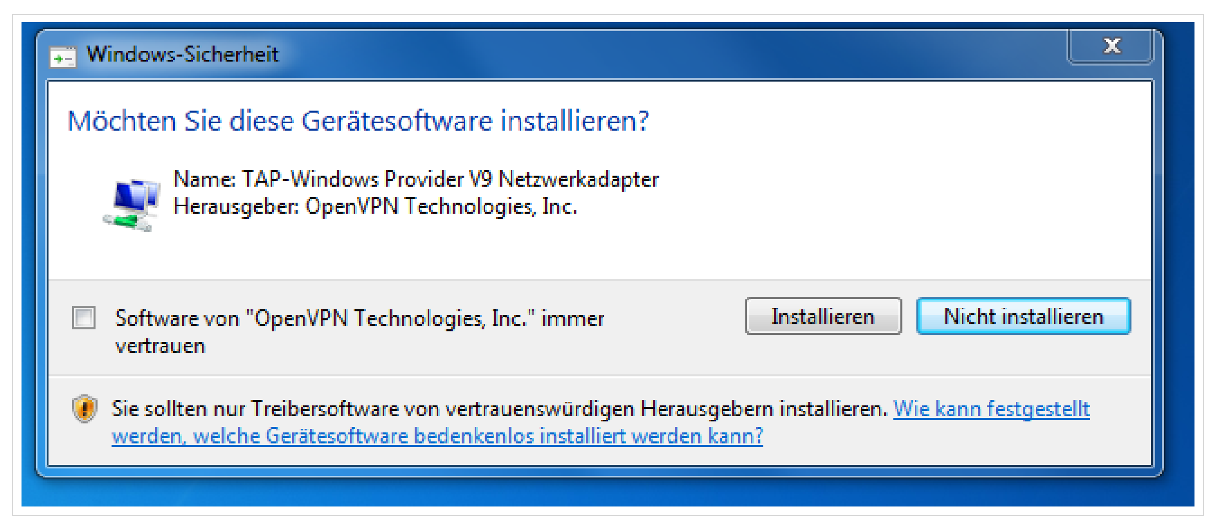


Abb. 282: Installation eines Netzwerkadapters für OpenVPN

---

[59] https://openvpn.net/index.php/open-source/downloads.html

Sobald das Programm installiert wurde, kann mit der Einrichtung begonnen werden. Hierfür benötigen Sie das im vorigen Abschnitt erwähnte Sicherheitszertifikat und die Konfigurationsdatei „*client.ovpn*“. Beide Dateien müssen Sie im Ordner *config* des OpenVPN-Installationsverzeichnisses ablegen.

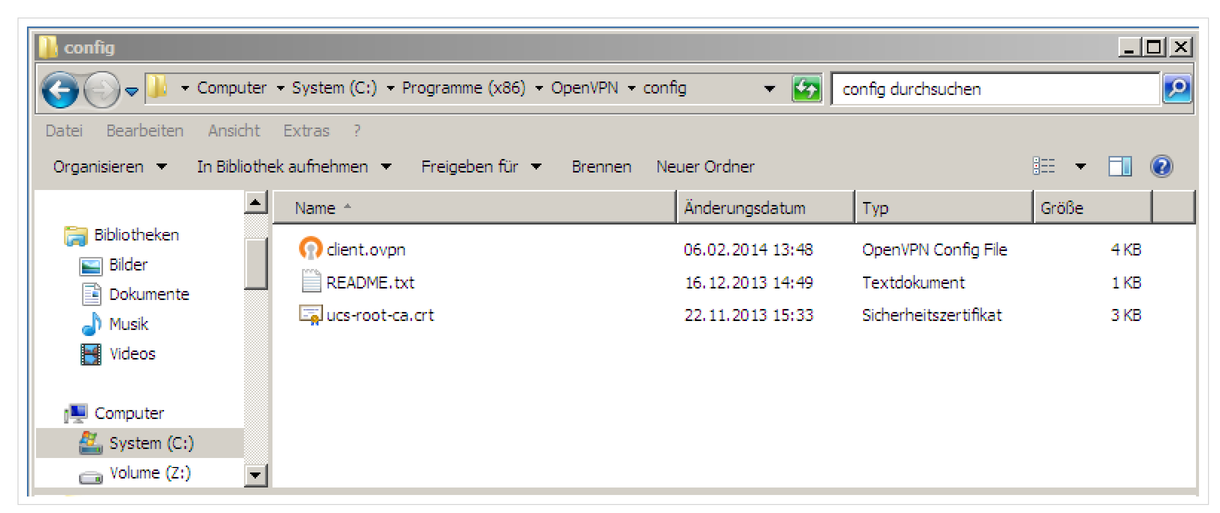


Abb. 283: Ordner mit Konfigurationsdatei und Zertifikat für den OpenVPN-Zugriff

Die Konfigurationsdatei sollte den folgenden Inhalt haben:

```
client
remote EXTERNE ADRESSE DES SCHULSERVERS
ca ucs-root-ca.crt
auth-user-pass
cipher AES-128-CBC
comp-lzo yes
dev tun
proto udp
auth-nocache
```

Statt des Eintrags „*EXTERNE ADRESSE DES SCHULSERVERS*“ muss Ihre feste IP-Adresse, bzw. der DDNS-Namen der Schule eingetragen werden. Sofern das Zertifikat anders heißen sollte, oder Sie das Zertifikat in einem anderen Ordner ablegen, müssen Sie den Wert „*ucs-root-ca.crt*“ in der dritten Zeile an Ihr System anpassen.

19.3.4 Herstellen einer OpenVPN-Verbindung

Das Programm *OpenVPN* versteckt sich – sobald es ausgeführt wird – als kleines Symbol unten links in der Taskleiste.



Abb. 284: Hinter diesem Symbol verbirgt sich OpenVPN

Um eine Verbindung mit dem Schulnetz herzustellen, führen Sie einen Klick mit der rechten Maustaste auf das Symbol aus. Es öffnet sich ein Menü. Wählen Sie die Verbindung (hier: „*client*“), die Sie herstellen wollen und navigieren Sie zu „*Verbinden*“.

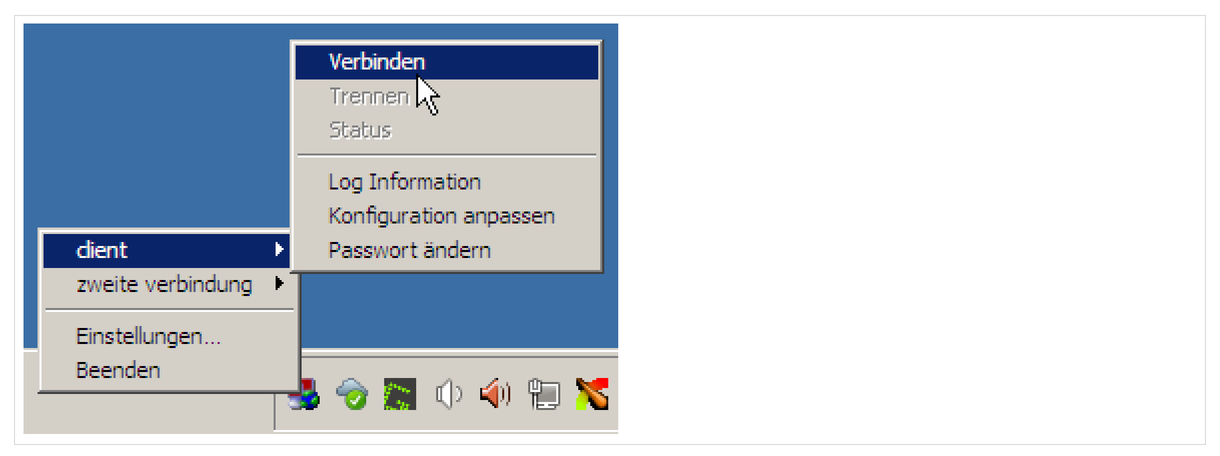


Abb. 285: Herstellung der Verbindung

Ein neues Fenster öffnet sich und Sie werden – sofern bis hier alle Einstellungen stimmen – nach Benutzername und Kennwort für das Schulnetz gefragt. Geben Sie hier die Zugangsdaten Ihres Schulnetzes ein.

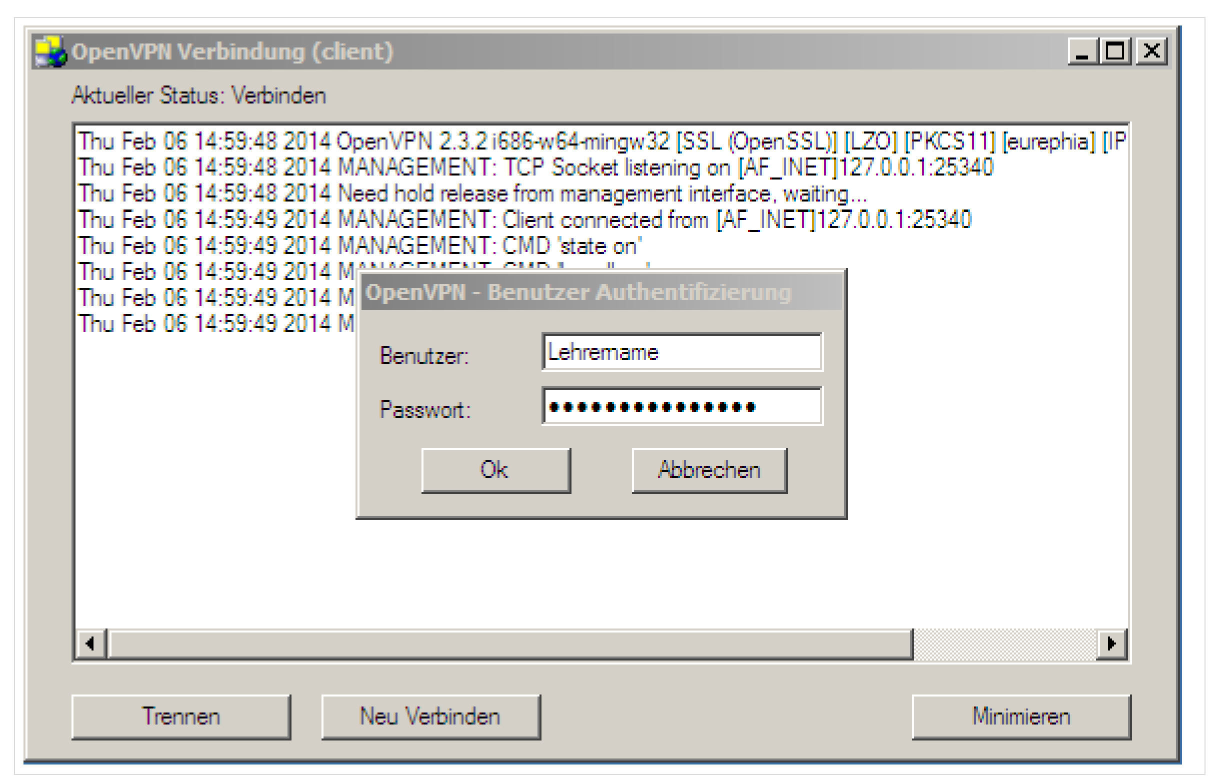


Abb. 286: Eingabe der Zugangsdaten

Sobald die Verbindung hergestellt wurde, wird das *OpenVPN*-Symbol der Taskleiste grün.



Abb. 287: alles im grünen Bereich

Sie haben nun Zugriff auf Dienste im Schulnetz und können dort alle internen Webseiten (zum Beispiel die Serverstartseite) aufrufen.

Wenn Sie einen *Windows*explorer öffnen, können sie nach der Eingabe von *server**BENUTZERNAME* – wobei *BENUTZERNAME* Platzhalter für Ihren Benutzernamen ist – auf Ihr Homeverzeichnis zugreifen und dort beispielsweise Unterrichtsmaterialien ablegen.

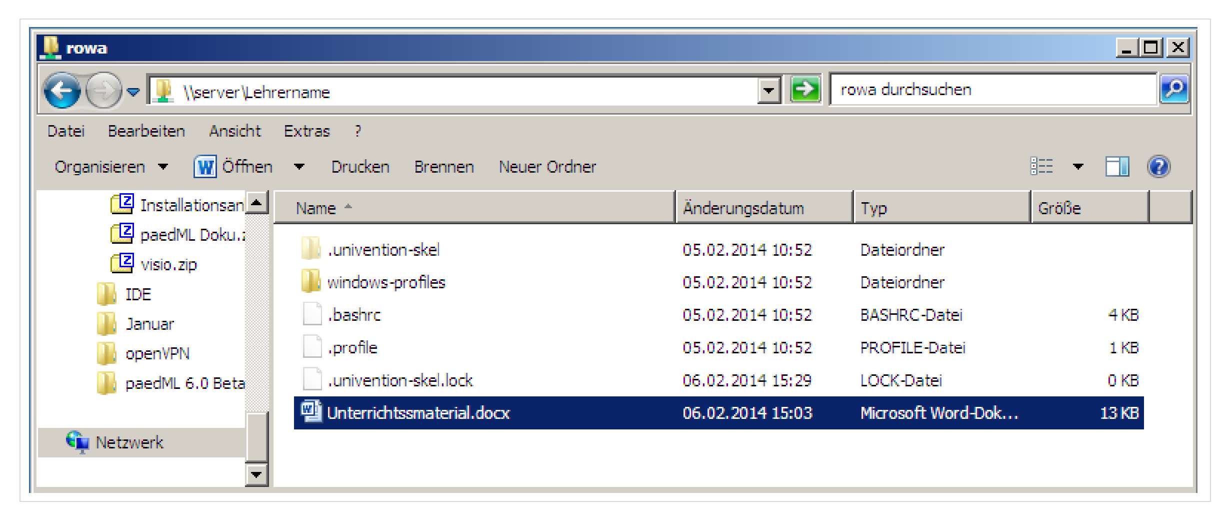


Abb. 288: Zugriff auf das eigene Homeverzeichnis via OpenVPN

20. Verzeichnisstruktur Nutzerdaten

Bei der Anmeldung an einem Rechner bekommen die Benutzer – abhängig von Ihrer Benutzerrolle (vgl. Kapitel 1.2, Seite 20) Freigaben des *paedML* Servers auf ihren Desktop eingebunden.

Hierbei handelt es sich um das Homeverzeichnis des angemeldeten Benutzers, Freigaben von Gruppen, deren Mitglied der Benutzer ist (z.B. Lehrer-Tauschverzeichnis – bei Lehrern, Arbeitsgruppen- und Klassentauschverzeichnisse – bei Schülern) sowie die Programmlaufwerk *K:* und das Laufwerk *Programme-S*[60].

Im Folgenden erhalten Sie eine Übersicht über die Verzeichnisse der *paedML Linux*, in denen Daten abgelegt werden. Es handelt sich hierbei um lokale Laufwerke, die Home-Verzeichnisse der Benutzer und um Tauschlaufwerke.

Verzeichnis	Inhalt
C:\	Lokale Festplatte Inhalte, die hier von Anwendern lokal abgelegt werden, werden nicht in das Benutzerprofil auf dem Server synchronisiert und gehen verloren!
H:\	Home-Laufwerk Benutzerdaten- und -profil
K:\	Laufwerk für die zentrale Installation von Programmen
T:\	Tauschlaufwerk (bei Lehrern: Lehrer-Tauschlaufwerk; bei Schülern: Klassen-Tauschlaufwerk)
Optional: Freigabe für alle beschreibbar	Kann bei Bedarf eingerichtet werden (s.u.)
Optional:	Weitere lokale Laufwerke (Festplattenpartitionen, Wechseldatenträger,…) Diese Laufwerke – und der Zugriff – sind abhängig von der Konfiguration der Arbeitsplatzrechner.

Tabelle 27: Laufwerke unter Windows

20.1 Anwendersicht auf Home-Verzeichnisse (H:\)



Home-Verzeichnisse von Benutzern werden auf dem Server erst angelegt, wenn sich Benutzer im System mindestens einmal angemeldet haben.

Vorher ist kein Zugriff auf diese Verzeichnisse möglich, da die Verzeichnisse nicht

[60] Dieses Laufwerk ist für alle Anwender sichtbar, muss aber – sofern Sie damit arbeiten wollen – gesondert eingerichtet werden (Vgl. Kapitel 20.5, Seite 241).

vorhanden sind.

Für jeden Benutzer der paedML Linux wird ein Home-Verzeichnis angelegt. Unter *Windows* wird das Laufwerk *H:* mit dem Homeverzeichnis des angemeldeten Benutzers verknüpft. Dabei werden die von *Windows* angelegten Ordner[61] in diesen Ordner umgeleitet. **Alle Daten, die nicht unter „H:\“ (bzw. in einem Tauschlaufwerk) gespeichert werden, werden gelöscht, wenn sich der Benutzer vom Rechner abmeldet.**

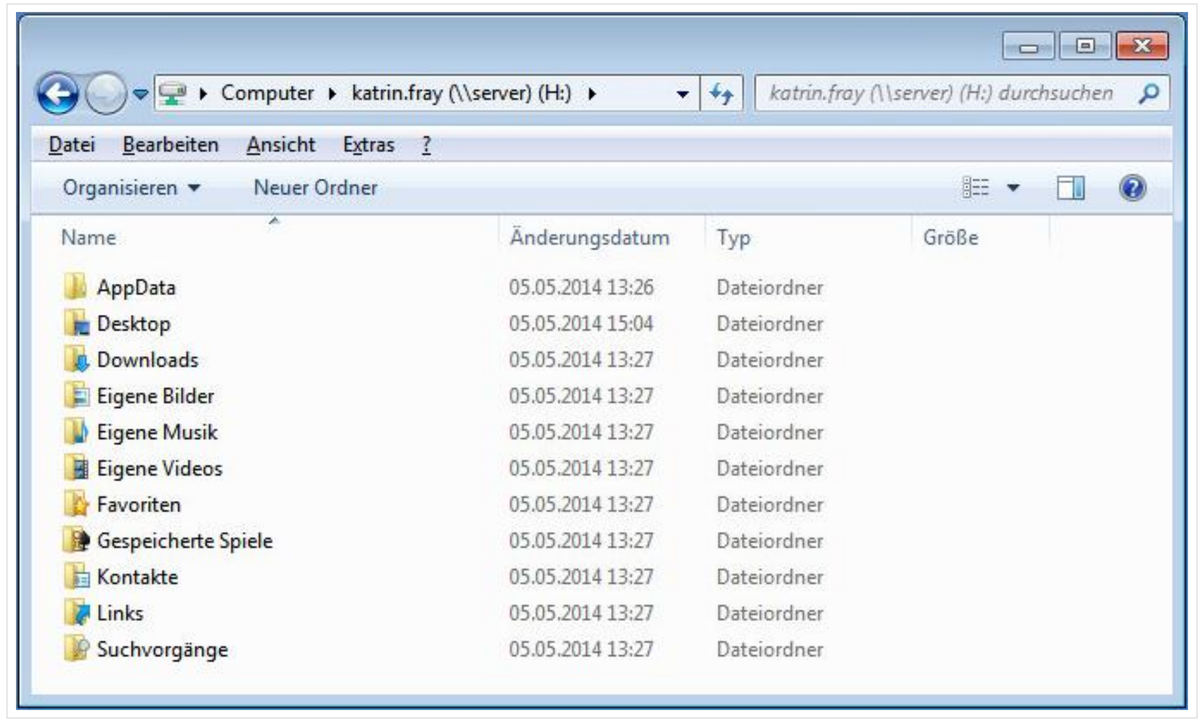


Abb. 289: Inhalt eines neu angelegten Home-Verzeichnisses

Der Zugriff auf *H:* kann für alle Benutzer alternativ über den Aufruf der Desktop-Verknüpfung „*Eigene Shares* | *Meine Dateien*“ erfolgen.

20.2 Administratorsicht auf /home

Sie finden auf dem *Server* die folgenden Verzeichnisse unter */home*:

Verzeichnisname	Inhalt
/home/Administrator	Home-Verzeichnis des Benutzers *Administrator*

[61] Hierbei handelt es sich ab *Windows* 7 um die sogenannten „special folders“ *Windows* inklusive dem „Desktop“ (vgl. http://de.wikipedia.org/wiki/Sonderverzeichnis).

	Windows-Freigabe *H:* Speichern Sie hier alle Dateien, die Sie als Administrator auch im Netz verfügbar haben wollen. **Alle Dateien von Administrator, die im eigenen Profil gespeichert werden, werden jeweils lokal auf dem Arbeitsplatz abgelegt und nicht auf den Server übertragen.**
/home/backup/BENUTZERNAME	Daten gelöschter Benutzer
/home/domadmin	**Der Benutzer domadmin sollte NUR für die Aufnahme von Clients in die Domäne genutzt werden!**
/home/groups */home/groups/klassen* */home/groups/schule-ARBEITSGRUPPENNAME*	Ablageort für Tauschverzeichnisse (vgl. nächster Abschnitt)
/home/groups/programme *Optional: /home/groups/programme-s*	Ablageort für Programme, die auf dem Server installiert werden (vgl. Seite 269 ff.)
/home/lehrer/NACHNAME.VORNAME	Home-Verzeichnisse der Lehrer Home-Verzeichnis des Benutzers *Windows-*Freigabe *H:*
/home/lost+found	Hier werden Dateien abgelegt, die vom System bei einer Überprüfung des Dateisystems mit dem Programm fsck gefunden aber keinem Benutzer zugeordnet wurden[62]
/home/netzwerkberater	Home-Verzeichnis des Benutzers „*netzwerkberater*“
/home/schueler/VORNAME.NACHNAME	Home-Verzeichnisse der Schüler Home-Verzeichnis des Benutzers *Windows-*Freigabe „*H:*“

Tabelle 28Verzeichnisse unter /home auf dem Server

[62] Im Normalfall ist dieses Verzeichnis leer.

20.3 Tauschverzeichnisse für Gruppen (T:\)

Die in der Schulkonsole angelegten Gruppen erhalten je ein Verzeichnis, in dem sich das Tauschlaufwerk der Gruppe befindet. Die Verzeichnisse liegen unter */home/groups*.

- */home/groups/klassen*
  - */home/groups/klassen/lehrer-schule* – Tauschverzeichnis der Lehrer
  - */home/groups/klassen/schule-KLASSENAME* – Klassentauschverzeichnis
- */home/groups/schule-ARBEITSGRUPPENNAME* – Tauschverzeichnis der Arbeitsgruppe

Der Zugriff auf die Tauschverzeichnisse erfolgt über die Verknüpfung „*Eigene Shares*“, die sich auf dem Desktop befindet.

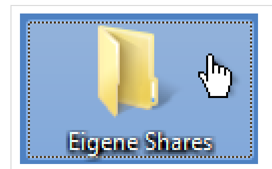


Abb. 290: Verknüpfung zu den Tauschlaufwerken

Die Inhalte der Verknüpfung sind – wie gesagt – abhängig von der Benutzerrolle. Sowohl Lehrer, als auch Schüler erhalten über die Verknüpfung „*Meine Dateien*“ Zugriff auf das eigene Homeverzeichnis und können über „pdfPrinterShare“ den PDF-Drucker einsehen (vgl. Kapitel 6.8, Seite 114).

Lehrer sehen die Klassen und Projekte, denen Sie zugeordnet sind und das Lehrer-Tauschverzeichnis.

Über den Link „*homes_schueler*“, der in „*Eigene_Shares*“ liegt“ gelangen Sie zu den Homeverzeichnissen aller Schüler.

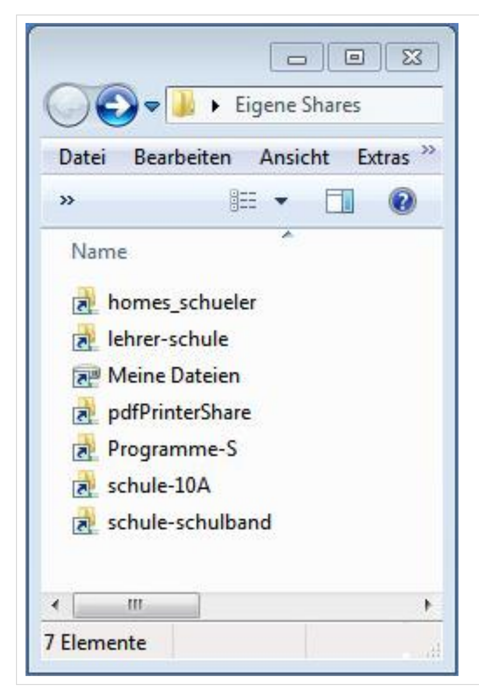


Abb. 291: Tauschlaufwerke eines Lehrers

Bei Schülern sind jeweils nur die eigene Klasse, sowie die Arbeitsgruppen sichtbar.

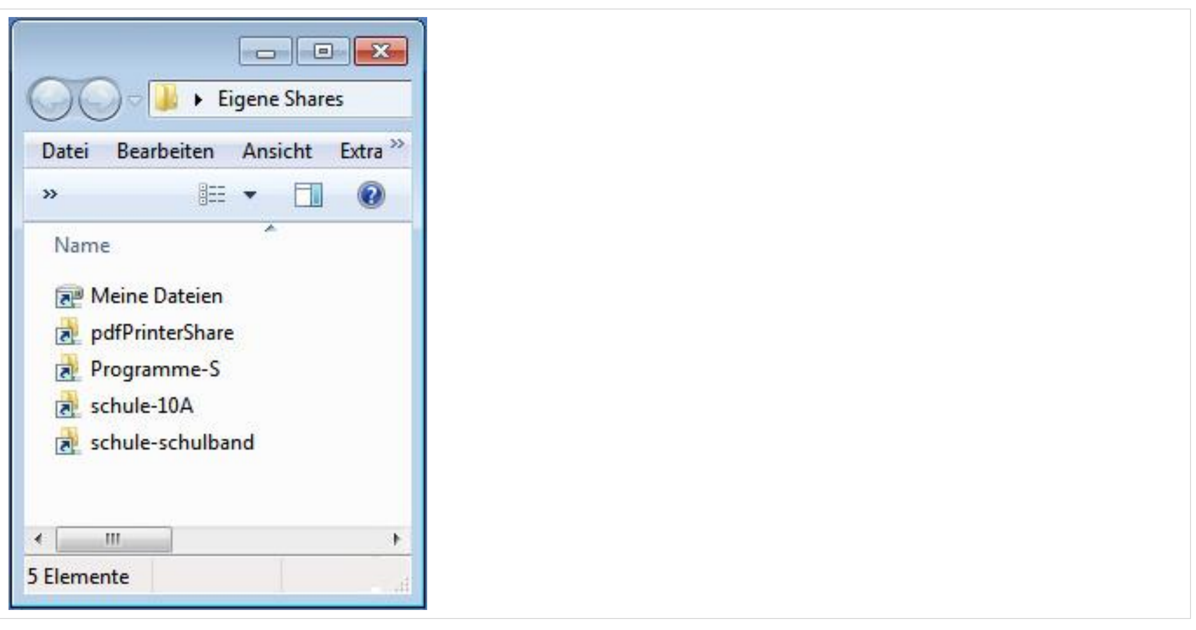


Abb. 292: Tauschlaufwerke eines Schülers.

Wenn die Computerübersicht aufgerufen wird, stellt sich das folgende Bild dar. Hierbei unterscheiden sich Schüler- und Lehrerprofile darin, dass über das Laufwerk *T:* bei Schülern das Tausch-Laufwerk der eigenen Klasse, bei Lehrern das Tauschlaufwerk der Gruppe Lehrer verfügbar ist.

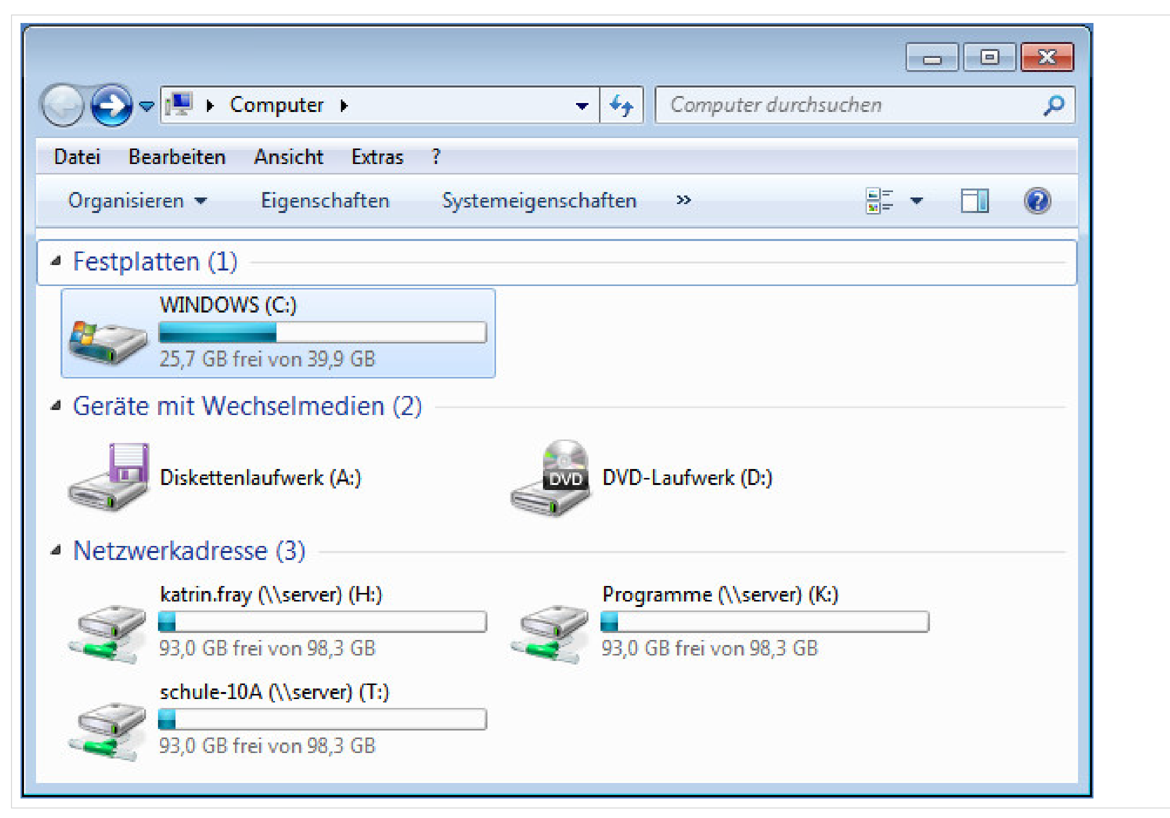


Abb. 293: Computerübersicht in einem Schüler-Profil.

20.4 Programmverzeichnis (K:\)

Unter */home/groups/programme* werden auf dem Server Programme abgelegt, die über das Netzwerk ausgeführt werden können. Hierdurch entfällt die Installation auf den Clients. Die Installation des Programmes muss nur einmal durchgeführt werden und die Images der Arbeitsplatzrechner bleiben schlank.

Nachteil dieser Installationsart ist, dass bei Ausführen der Programme Last auf dem Netzwerk entstehen kann. Insbesondere wenn mehrere Nutzer gleichzeitig Programme auf dem Server ausführen.

Schreibenden Zugriff auf den Programme-Ordner hat die Gruppe „admins-schule“, also die Benutzer *netzwerkberater* und *Administrator*.

Wenn Sie ein Programm auf *K:* installieren wollen, dann wählen Sie dieses Laufwerk als Installationsort während der Installationsroutine des Programmes aus.

Geben Sie als Installationspfad den UNC-Pfad der Verknüpfung „*Programme*“, sowie einen Namen für das Programm ein. Am Beispiel der Installation von Gimp-Portable ist der UNC-Pfad, in den das Programm installiert wird *\\server\Programme\gimp2*.

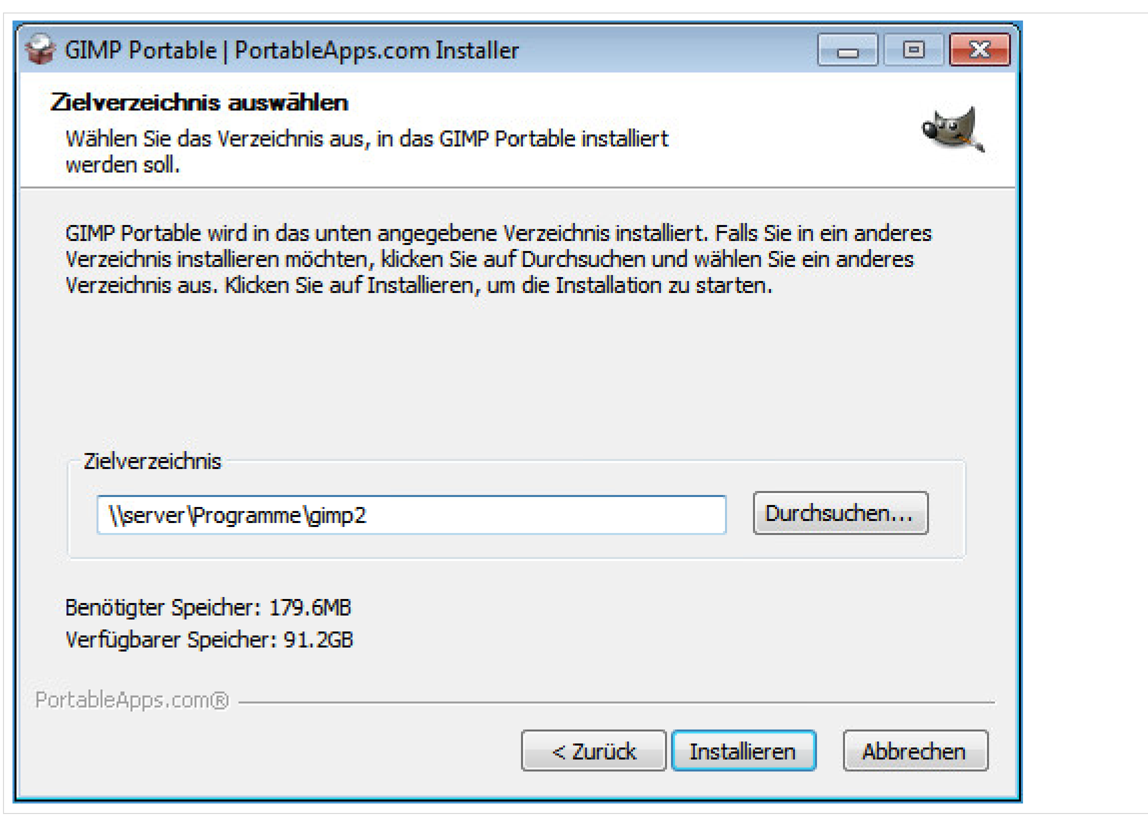


Abb. 294: Installation nach Programme (K:\)

In K:\ installierte Programme sind für alle Domänenbenutzer verfügbar.



Damit ein Programm über das Programmlaufwerk verfügbar gemacht werden kann, muss es die Netzwerkinstallation unterstützen.

Viele Programme benötigen eine lokale Installation um lauffähig zu sein!

20.5 Für alle beschreibbares Share

Unter */home/groups/programme-s* gibt es einen Ordner, der für alle Domänenbenutzer beschreibbar frei gegeben werden kann.

Hintergrund hierfür ist, dass es Programme gibt, die nur dann ausgeführt werden können, wenn der ausführende Benutzer auch Schreibzugriff auf den Installationsordner des Programmes hat. Ein prominentes Beispiel aus der Grundschule ist das Programm „*Lernwerkstatt*“.

Eine Standardinstallation in das Laufwerk *K:* würde verhindern, dass Schüler mit dem Programm arbeiten können, da sie keine Schreibrechte für die Freigabe haben.



Ein für alle Anwender beschreibbares Share hat nicht nur Vorteile:

- Neben nützlichen Dateien kann hier jeder Anwender auch unnütze Daten ablegen. Dieses Verzeichnis sollte regelmäßig aufgeräumt werden!
- Wenn alle Benutzer schreibend auf das Verzeichnis zugreifen können, dann können sie Daten auch (vorsätzlich oder versehentlich) löschen. Sie sollten das Verzeichnis ggf. gesondert sichern, um die Daten schnell wieder herstellen zu können.

Das für alle beschreibbare Verzeichnis ist im Auslieferungszustand nicht eingerichtet.

Um das Laufwerk einzurichten, melden Sie sich als Benutzer *Administrator* an der *Schulkonsole* an. Navigieren Sie in das Menü „*Domäne*“ und wählen Sie dort den Eintrag „*Freigaben*“.

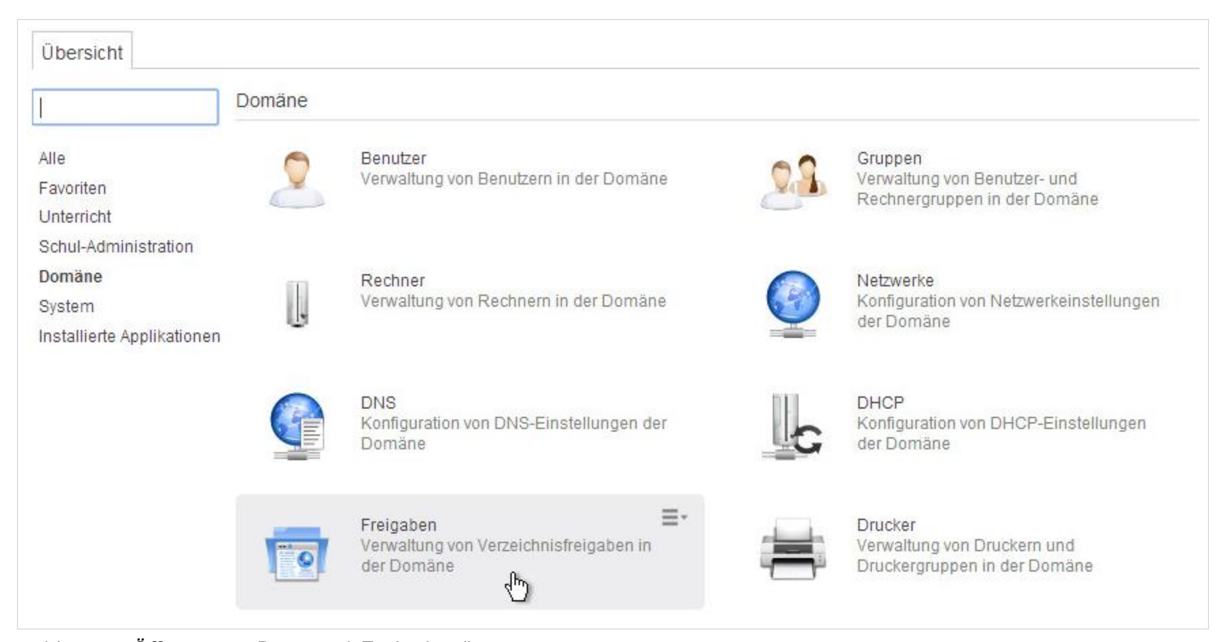


Abb. 295: Öffnen von „Domäne | Freigaben“

Es öffnet sich eine Liste mit allen im System eingerichteten Freigaben. **Hier darf außer dem beschriebenen Eintrag KEINE ÄNDERUNG vorgenommen werden!** Navigieren Sie zum Eintrag

„Programme-S (/home/groups/programme-s…)“ und wählen Sie die Freigabe durch das Aktivieren der Checkbox vor dem Eintrag (grüner Haken). Klicken Sie anschließend auf das „*Bearbeiten*“-Symbol, das Sie oberhalb des Fensters mit den Freigaben finden können.

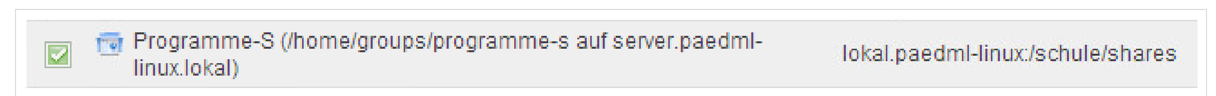


Abb. 296: Ändern der Freigabe „Programme-S“

Es öffnet sich ein neues Fenster, das verschiedene Reiter enthält. Die Aktivierung der Freigabe geschieht über den Reiter „*Samba*“. Die erste (nicht aktivierte) Checkbox für den Eintrag „*Samba-Schreibzugriff*“ muss aktiviert werden, damit der Schreibzugriff für alle Benutzer aktiviert wird.

Klicken Sie anschließend auf „*Änderungen speichern*“.

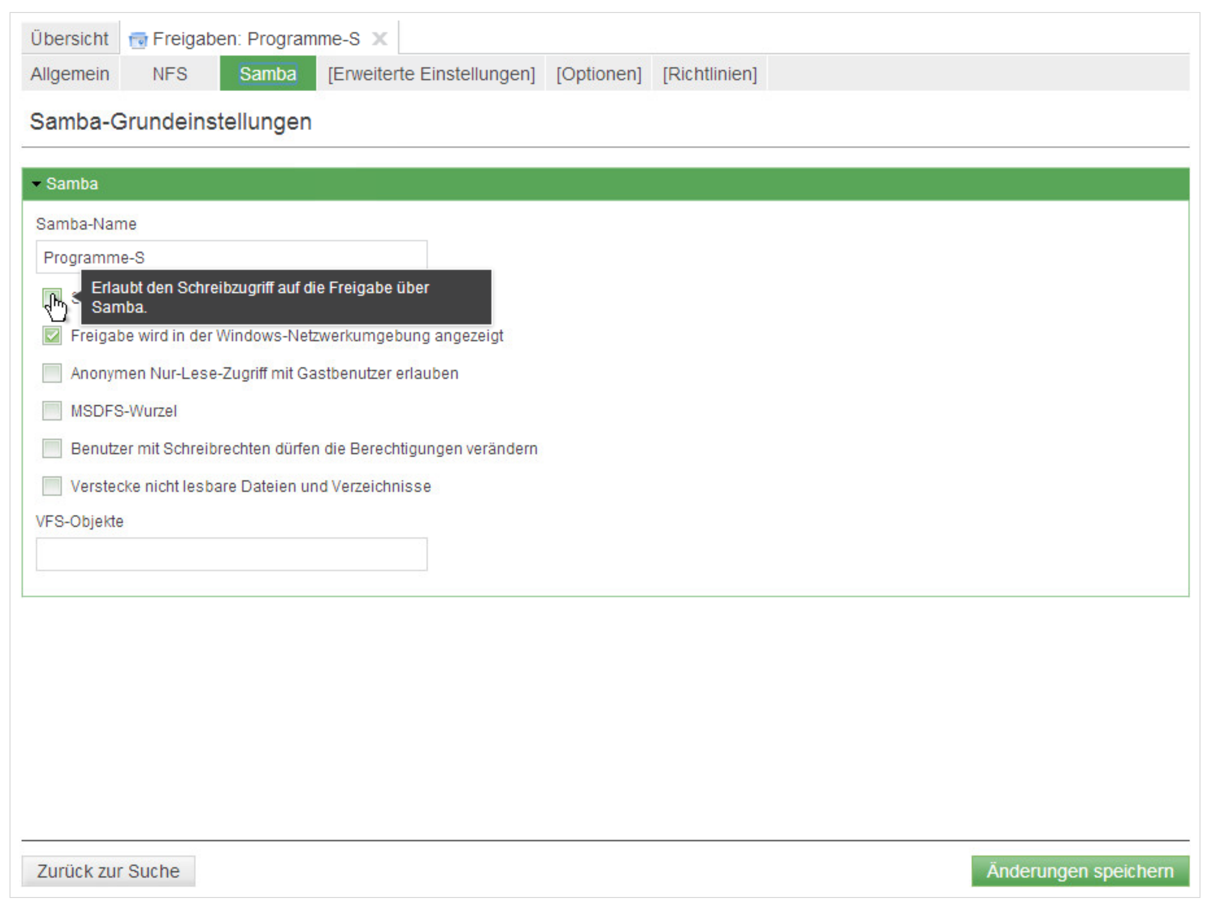


Abb. 297: Aktivieren des Wertes „Samba-Schreibzugriff“

Wenn diese Änderungen durchgeführt werden, dann können alle Benutzer – nach einer Neuanmeldung am *Windows*-Rechner auf das Verzeichnis *Programme-S* zugreifen, nachdem sie auf den Link „*Eigene Shares*“ auf dem Desktop geklickt haben.

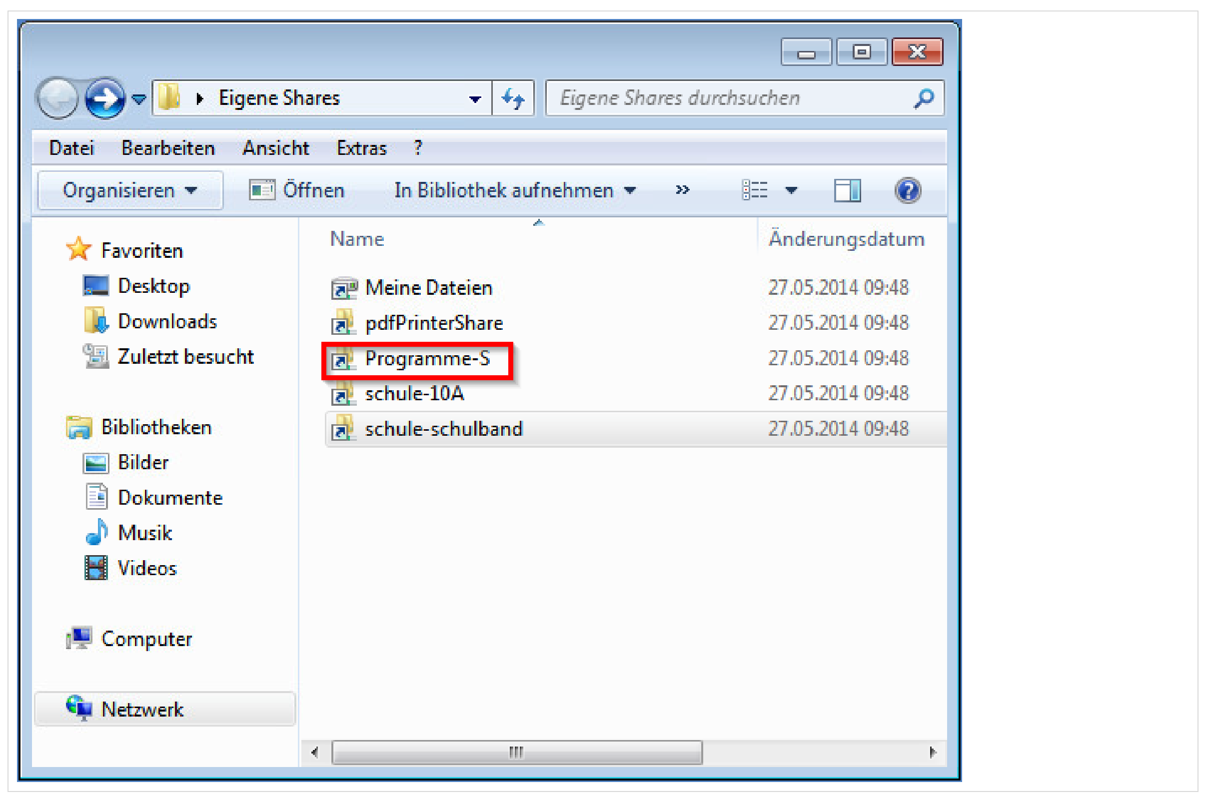


Abb. 298: Programme-S kann aufgerufen werden, wenn es aktiviert wurde.

Die Installation in die Freigabe „*Programme-S*“ erfolgt analog zur Installation von Software in das Programmlaufwerk K:\ (vgl. Kapitel 20.4, Seite 269). Geben Sie als Installationspfad den UNC-Pfad der Verknüpfung „*Programme-S*“, sowie einen Namen für das Programm ein. Am Beispiel der Installation von Gimp-Portable ist der UNC-Pfad, in den das Programm installiert wird *\\server\Programme-S\gimp2*.

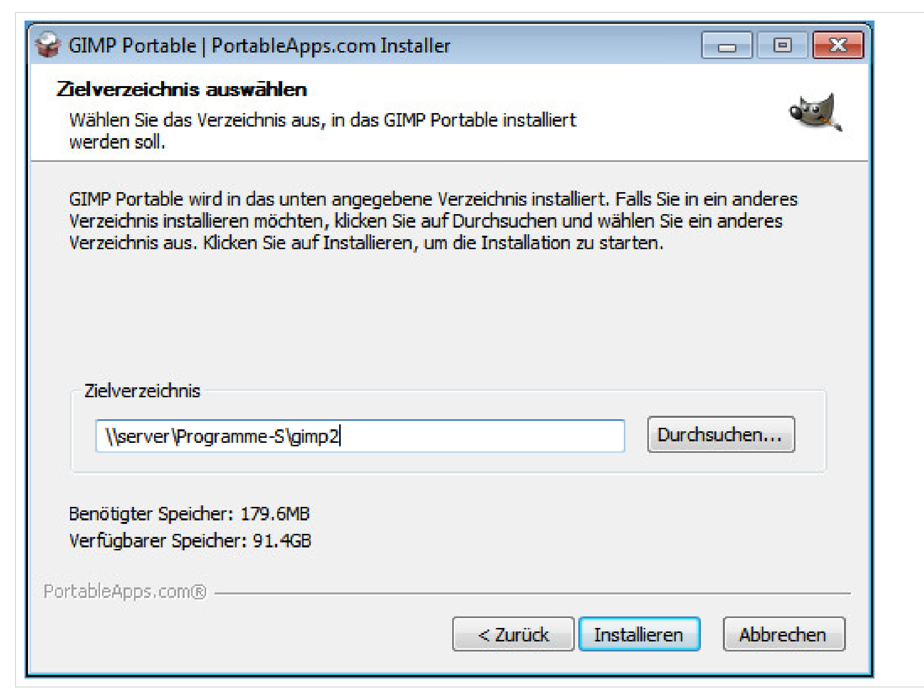


Abb. 299: Installation nach Programme-S

21. Datensicherung und Datenwiederherstellung

Adresse: https://server.paedml-linux.lokal/backuppc

21.1 Grundsätzliche Überlegungen

Bevor wir in die technischen Details der Backuplösung der paedML Linux einsteigen, wollen wir kurz ein paar konzeptionelle Überlegungen anstellen. Vertiefen Sie dieses Thema mit Ihrem Dienstleister, der Sie in puncto Datensicherung beraten kann.

Dem Thema Datensicherung geht zunächst immer die Frage voraus: „Für oder gegen was schütze ich mich?". Folgende Szenarien sind denkbar, in denen Daten „abhanden" kommen können:

- Probleme mit der Hardware
  - Physikalischer Defekt (Ausfall der Hardware)
  - Zerstörung der gesamten Infrastruktur (Elementarschaden, Stromschaden,…)
  - Diebstahl von Hardware
- Probleme mit Anwendungen
  - Datenverlust durch Softwarefehler („Datei kaputt")
- Probleme mit Anwendern
  - Versehentliches/mutwilliges Löschen von Anwendungsdaten durch Benutzer

Die verschiedenen Szenarien erfordern verschiedene Ansätze, damit die Sicherung von Daten gegen den Verlust umgesetzt werden kann.

1. Im Fall von Beschädigung oder Verlust der Hardware sollte gewährleistet sein, dass Backupsätze nicht ebenfalls betroffen sind. Antworten darauf wären beispielsweise
   1.1. die Auslagerung von Backupdiensten auf eigene Hardware und/ oder
   1.2. die Auslagerung der Backup-Hardware an einen anderen Ort (Stichwort „onsite/offsite backup").
2. Im Fall von „einfachem" Datenverlust durch Löschung von Daten oder Softwarefehler genügt es sicherlich, die Daten aus dem Produktivsystem wegzusichern. Hierfür würde es ausreichen, eine weitere virtuelle Maschine aufzusetzen, auf der ein Datensicherungsserver läuft[63]. Es gibt auch Open-Source Distributionen, wie z.B. FreeNAS[64], die als Datensicherungssystem kostengünstig eingerichtet werden können.

„Paranoide" Backupkonzepte, die durchaus Sinn ergeben, gehen noch einen Schritt weiter: Der regelmäßige Austausch des Backupmediums soll dafür sorgen, dass ein defekter Datenträger, auf dem gesichert wurde, nicht als weitere Problemquelle bei der Wiederherstellung auftritt. Wenn diese

---

[63] Diese Variante ist sicherlich kostengünstig, aber aus genannten Gründen nur bedingt „sicher". Auf jeden Fall sollten die Backup-Daten auf einer anderen physikalischen Platte lagern als die Nutzdaten, besser noch auf einem anderen System und nicht auf dem gleichen ESXi-Server wie das Produktivsystem!

[64] http://www.freenas.org/

ausgetauschten Datenträger nicht im Serverraum gelagert werden, ist zudem die Wahrscheinlichkeit, das Produktivsystem und Backupdaten zeitgleich unbrauchbar werden, geringer. Möglicherweise genügt es auch schon, die Datenträger im Schulsafe zu hinterlegen.



Achten Sie nach Möglichkeit darauf, dass Backupkonzepte so aussehen sollten, dass Sicherungen nicht nur vor Ort vorgehalten werden, sondern Sie regelmäßig die gesicherten Daten vom Sicherungssystem abziehen und an einem anderen Ort aufbewahren.

Bei Diebstahl von Hardware aus dem Serverraum oder bei Beschädigung der Hardware (Brand, Wasserschaden,…) ist ein lokales Vorhalten von Sicherungsdaten unter Umständen unzureichend.

21.2Das Backupkonzept der paedML Linux 6.0

Mit der *paedML Linux 6.0* hält das einfach zu bedienende Backupprogramm *BackupPC* Einzug in die Welt der *paedML*.

Die *paedML Linux* ist so weit vorkonfiguriert, dass ein Backup-Device, welches gemäß dieser Anleitung eingerichtet worden ist, „out of the box" zur Datensicherung herangezogen wird.

Gesichert werden Daten der folgenden *paedML Linux*-Maschinen

- Server
- Backup-Server (opsi-Server)
- Firewall (pfSense)

Sie können die Oberfläche von *BackupPC* direkt über die Adresse: https://server.paedml-linux.lokal/backuppc oder über die Serverstartseite über den Reiter „*Administration*" und die Schaltfläche „*BackupPC Management*" erreichen.

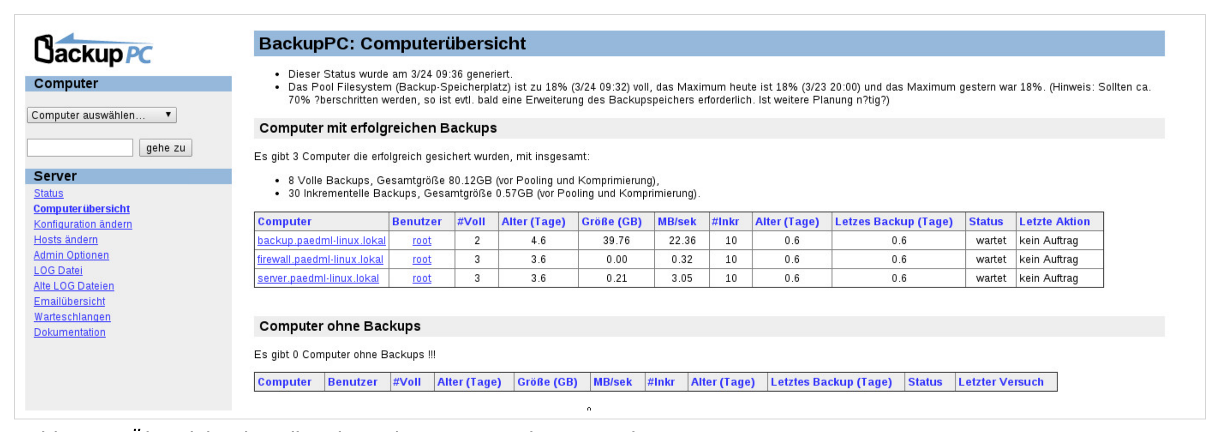


Abb. 300: Übersicht über die mit BackupPC verwalteten Rechner

21.2.1 Sicherungsintervall

Die paedML Linux legt wöchentlich (freitags) ein Vollbackup der Daten an. An allen anderen Tagen der Woche werden inkrementelle Sicherungen erstellt, in denen die seit der letzten Sicherung (Vollbackup

oder inkrementelle Sicherungen) geänderten Daten gesichert werden. Die Sicherungen werden jeweils um 20.00 Uhr angestoßen.

Es werden jeweils bis zu drei Vollbackups und bis zu 30 inkrementelle Datensicherungen vorgehalten.

Art der Sicherung	Wochentage	Uhrzeit	vorgehaltene Datensätze
Vollbackup	freitags	20	3
Inkrementelles Backup	samstags - donnerstags	20	30

Tabelle 29: Backupzeiten

21.2.2 Inhalte der Datensicherung

Die Datensicherung umfasst die für den Betrieb der paedML notwendigen Daten. Hierzu gehören

- Serverdaten des Servers
  - OpenLDAP-Dump (/var/univention-backup)
  - UCR-Dump (/var/univention-backup)
  - Samba LDAP-Verzeichnis, Samba Logonscripte (/var/lib/samba und /var/lib/samba/sysvol/paedml-linux.lokal)
  - Konfigurationsdateien/Templates (/etc)
  - Benutzerdaten (/home)
  - Horde-Einstellungen (PostgreSQL hordedb-Datenbank)
  - Maildaten und Seen-Datenbanken (/var/spool/cyrus und /var/lib/cyrus)
- Serverdaten des Backup-Servers
  - UCR-Dump (/var/univention-backup)
  - Konfigurationsdateien/Templates (/etc)
  - opsi-Depot und opsi-Einstellungen (/var/lib/opsi und /var/lib/opsi/config)
- Firewall
  - Firewall-Einstellungen (/cf)
  - Firewall-Default-Einstellungen (/conf.default)

21.3 Einrichtung des Backupsystems (NAS)



Die Konfiguration von BackupPC ist so eingerichtet, dass Datensicherungen angelegt werden, sobald eine NAS unter den hier beschriebenen Vorgaben eingerichtet und mit dem Server verbunden wurde.

Es ist derzeit nicht vorgesehen, dass in der Datensicherung andere Systeme als die hier beschriebenen abgebildet werden. Ferner unterstützt die Hotline derzeit keine Anpassungen am System der Datensicherung. Wenn Sie an der Konfiguration von *BackupPC* Änderungen vornehmen wollen, so geschieht dies auf eigene Gefahr.

Wenn Sie konkrete Wünsche oder Verbesserungsvorschläge haben, wie unser Datensicherungssystem angepasst werden kann, dann kontaktieren Sie uns bitte diesbezüglich.

> Die Einrichtung und Wartung der NAS ist Aufgabe des Dienstleisters. Die Mitarbeiter der Hotline können höchstens unterstützend wirken.
>
> **Zur Sicherung der paedML-Daten benötigen Sie eine NFS-fähige NAS[65]!**

Es kann keine allgemein gültige Aussage über die Hardwareanforderungen gemacht werden. Für eine Schule mit 200 Benutzern ist der Speicherplatzbedarf geringer als für eine Schule mit 800 oder sogar 2000 Benutzern.

Faktoren, wie die Verfügbarkeitsanforderungen und die Größe der zu sichernden Daten, spielen maßgeblich in die Auswahl einer Backup-NAS hinein.

Zunächst sollte die zu erwartende Datenmenge ermittelt werden. Hierbei muss berücksichtigt werden, dass – je nach Konfiguration – Datensicherungen mehrfach mit verschiedenen Ständen vorgehalten werden sollten.

Neben der Datenmenge muss auch die Wichtigkeit der Daten abgewogen werden.

Eine sehr kleine und somit günstige NAS kann im Normalfall zwischen zwei und vier Festplatten aufnehmen. In größeren Umgebungen kommen solche Systeme zum einen bezogen auf die

Speicherkapazität zum anderen bezogen auf die verfügbaren Ressourcen (Durchsatz des RAID-Controllers, Netzwerkschnittstelle etc.) sehr schnell an ihre Grenzen.

Es muss auch beachtet werden, dass der gewählte RAID-Level sowohl über verfügbaren Speicherplatz als auch die Datensicherheit bestimmt.

RAID5 beispielsweise verkraftet nur eine defekte Festpatte, RAID6 hingegen zwei.

Beim Einsatz von RAID5 steht jedoch mehr Speicherplatz als bei RAID6 zur Verfügung.

Bei extrem geringen Datenmengen könnte auch RAID1 zum Einsatz kommen.

Um bei einem Plattenausfall den sofortigen Rebuild des RAID-Verbunds zu ermöglichen, kann eine Spare-Platte zum Einsatz kommen.

Es empfiehlt sich, die Anforderungen an das System genau zu prüfen. Werden die Anforderungen nicht ausreichend geprüft, kann sich das sehr schnell durch mangelnde Ressourcen oder Speicherplatzmangel rächen.

Auf folgende Punkte sollte zwingend geachtet werden:

- Die NAS muss NFS bereitstellen,
- die NAS sollte NFS-File-Lockings[66] unterstützen, da andernfalls Race Conditions[67] die Folge sein können und

---

[65] Vgl. https://de.wikipedia.org/wiki/Network_Attached_Storage

[66] Durch File-Locking wird der Zugriff auf Dateien so geregelt, dass immer nur ein Prozess/Benutzer gleichzeitig auf eine Datei (schreibend) zugreifen kann.

- der Durchsatz des RAID-Controllers sollte ausreichend dimensioniert sein, da andernfalls Performanceprobleme die Folge sind und – je nach Datenmenge – Full-Backups länger als 24 Stunden brauchen könnten.

In der NAS, die für die Datensicherung benötigt wird, sollten folgende konfigurative Anpassungen vorgenommen werden.

Parameter	Wert
IP-Adresse	10.1.0.12/24
Hostname:	nas-backup.paedml-linux.lokal
DNS-Server (optional)	10.1.0.1
Gateway (optional)	10.1.0.11
Share "backuppc" einrichten Zugriffsbeschränkung auf IP-Adresse des Servers setzen (empfohlen)	/mnt/backuppc
ID Mapping	Stammkonto des Gastsystems hat vollen Zugriff (root:root)

Tabelle 30: Parameter der NAS für die Datensicherung

21.4Wiederherstellen von Daten

Das Wiederherstellen von Daten geschieht mit wenigen Mausklicks. Sie öffnen die Benutzer-Oberfläche von *BackupPC* und wählen auf der linken Seite im Abschnitt „*Computer*“ das System, dessen Daten Sie wiederherstellen wollen.

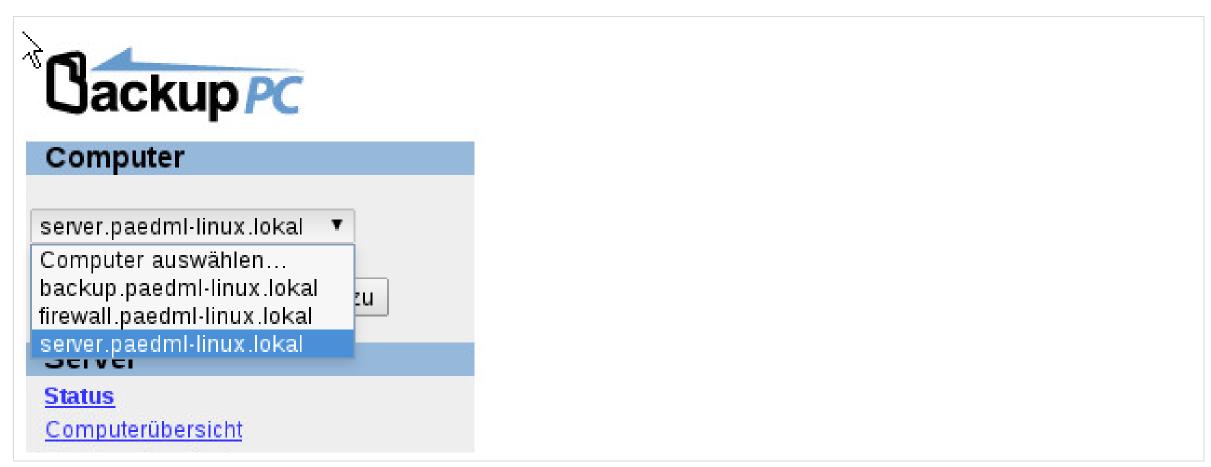


Abb. 301: Welches System soll wiederhergestellt werden?

[67] Programmfehler, die beim gleichzeitigen Zugriff auf Daten entstehen können (vgl. http://de.wikipedia.org/wiki/Race_Condition).

In der folgenden Ansicht klicken Sie auf „*Datensicherungen anzeigen*“, um Zugriff auf die Backupdaten zu erhalten.



Abb. 302: Anzeigen von Datensicherungen

Anschließend navigieren Sie im Hauptfenster in das Verzeichnis der Datensicherung, in dem die wiederherzustellenden Daten abgelegt wurden. Im oberen Drittel des Fensters finden Sie ein Dropdown-Menü (roter Pfeil), über das Sie den Backupdatensatz aussuchen können. Sie können einzelne oder mehrere Dateien sowie ganze Verzeichnisse wiederherstellen. Markieren Sie die Checkboxen vor den Dateien und klicken Sie auf „*Selektion wiederherstellen*“.

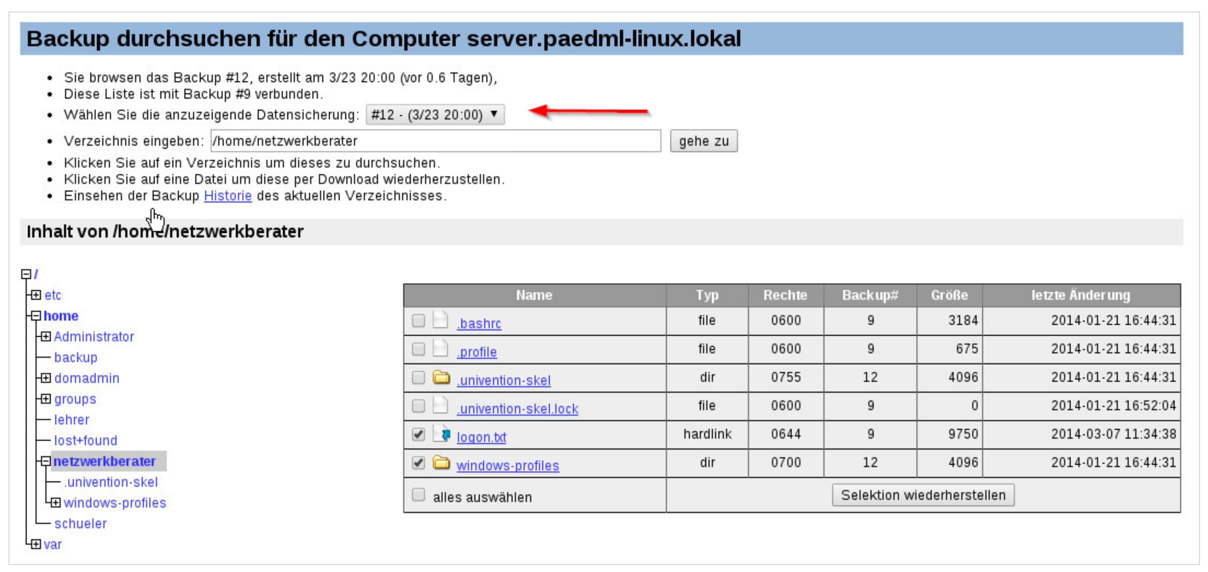


Abb. 303: Auswahl der Daten

Das Wiederherstellen der Daten kann direkt in das entsprechende Verzeichnis oder in ein herunter-ladbares Archiv durchgeführt werden. Letzteres hat den Vorteil, dass die Daten lokal auf dem

Arbeitsplatz, auf dem Sie die Daten wieder hergestellt haben, bearbeitet oder auf einen USB-Stick gespielt werden können.

Im Fall der Wiederherstellung der Daten auf dem Zielsystem müssen Sie das Überschreiben der Daten bestätigen.

Restore Optionen für server.paedml-linux.lokal

Sie haben die folgenden Dateien/Verzeichnisse aus der Freigabe / des Backups mit der Nummer #12 selektiert:

- /home/netzwerkberater/logon.txt

Sie haben drei verschiedene Möglichkeiten zur Wiederherstellung (Restore) der Dateien/Verzeichnisse. Bitte wählen Sie eine der folgenden Möglichkeiten:.

Möglichkeit 1: Direkte Wiederherstellung

Sie können diese Wiederherstellung starten um die Dateien/Verzeichnisse direkt auf den Computer **server.paedml-linux.lokal** wiederherzustellen. Alternativ können Sie einen anderen Computer und/oder Freigabe als Ziel angeben.

Warnung: alle aktuell existierenden Dateien/Verzeichnisse, die bereits vorhanden sind, werden überschrieben! (Tip: Alternativ eine spezielle Freigabe erstellen mit Schreibrecht für den Backup-Benutzer und die wiederhergestellten Dateien/Verzeichnisse durch Stichproben prüfen, ob die beabsichtigte Wiederherstellung korrekt ist.)

Restore auf Computer: server.paedml-linux.lokal
Restore auf Freigabe: /
Restore in Unterverzeichnis (relativ zur Freigabe): /home/netzwerkberater
[Wiederherstellung starten]

Möglichkeit 2: Download als Zip Archiv

Sie können eine ZIP Archivdatei downloaden, die alle selektierten Dateien/Verzeichnisse enthält. Mit einer lokalen Anwendung (z.B. WinZIP, WinXP-ZIP-Ordner...) können Sie dann beliebige Dateien entpacken.

Warnung: Abhängig von der Anzahl und Größe der selektierten Dateien/Verzeichnisse kann die ZIP Archiv Datei extrem groß bzw. zu groß werden. Der Download kann sehr lange dauern und der Speicherplatz auf Ihrem PC muß ausreichen. Selektieren Sie evtl. die Dateien/Verzeichnisse erneut und lassen sehr große und unnötige Dateien weg.

☑ Archiv relativ zu Pfad /home/netzwerkberater (andernfalls enthält die Archiv Datei vollständige Pfade).
Kompression (0=aus, 1=schnelle,...,9=höchste) 5
[Zip Datei downloaden]

Möglichkeit 3: Download als Tar Archiv

Abb. 304: Auswahlmöglichkeiten für Datenwiederherstellung

21.5 LOG-Dateien

Bei jedem Sicherungsvorgang werden Log-Dateien angelegt, die Sie über die Maske von *BackupPC* einsehen können. Drücken Sie hierfür auf den entsprechenden Eintrag im Navigationsmenü auf der linken Seite. Über den Eintrag „*LOG Datei*" bekommen sie die letzte Log-Datei angezeigt. Der Menüpunkt „*Alte LOG Dateien*" führt Sie zu einer Ansicht alter Log-Dateien.

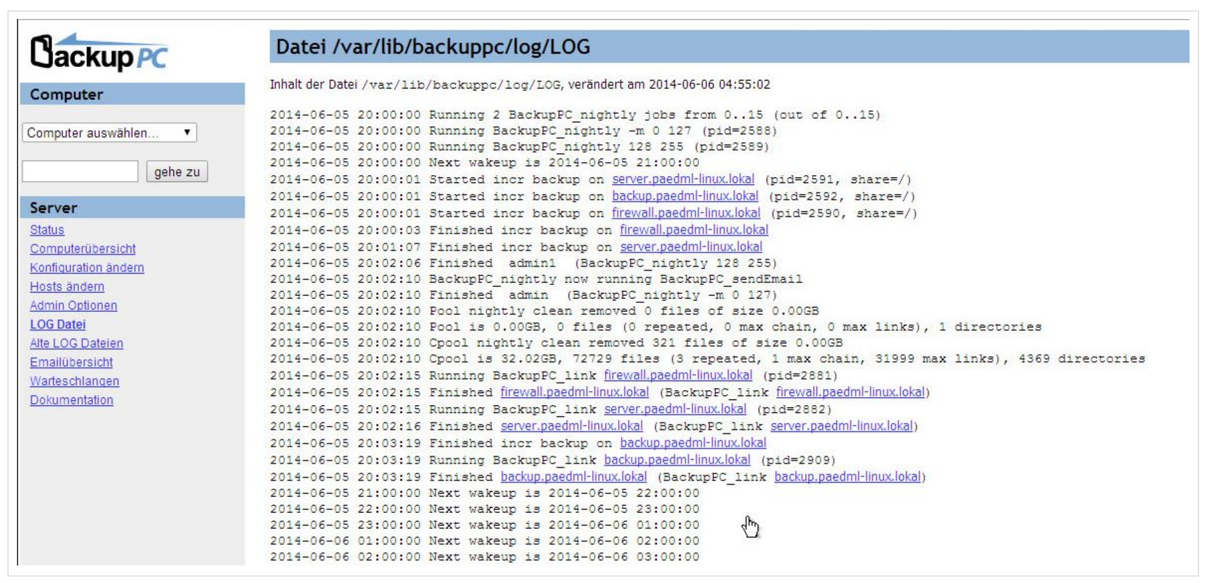


Abb. 305: Log-Datei von BackupPC

22. Fernzugriff zur Wartung

Der Fernzugriff durch die Mitarbeiter der Linux-Hotline erfolgt über das Programm *Teamviewer*. Durch *Teamviewer* kann – ohne Einrichtung von Firewallregeln – direkt aus dem Internet auf einen Rechner zugegriffen und eine Fernwartung durchgeführt werden.

Das Programm liegt als *opsi*-Paket vor und kann über *opsi* installiert werden oder Sie können es unter www.teamviewer.com herunterladen und auf den fern zu steuernden Rechner ausspielen.



Die Software *Teamviewer* ist NUR für den privaten Gebrauch kostenlos. Für die kommerzielle Nutzung – und hierzu zählt auch der Einsatz in der Schule – muss eine Lizenzgebühr an den Hersteller abgeführt werden. Der kostenlose Zugriff auf Services des Schulnetzes kann über *OpenVPN* umgesetzt werden (vgl. Kapitel 19, Seite 255).



Abb. 306: Teamviewer kann als opsi-Paket installiert werden



Im Idealfall betreiben Sie einen *Management-PC* (Vgl. Kapitel 1.1.7, Seite 19), auf dem *Teamviewer* installiert wird.

Hierdurch bekommt die Hotline die Möglichkeit direkt auf die unter *VMware* laufenden Maschinen, sowie bei Bedarf auch auf die Virtualisierungsschicht zuzugreifen.

Alternativ kann *Teamviewer* auch auf der *AdminVM* installiert werden. Hierdurch bekommen die Hotline-Mitarbeiter Zugriff auf Dienste, die auf der *AdminVM* laufen (z.B. *VAMT*). Über die *AdminVM* kann ein Zugriff auf *opsi* und die *Schulkonsole* hergestellt werden.

22.1 Zugriff auf Teamviewer

Nachdem *Teamviewer* installiert wurde, können Sie das Programm auf dem fernzusteuernden Rechner ausführen.

Das Hauptfenster des Programmes zeigt eine ID und ein zugehöriges Kennwort. Mit diesen Daten kann eine Remote-Verbindung zu dem Rechner aufgebaut werden. Das Kennwort ändert sich, sobald das Programm neu gestartet wird.

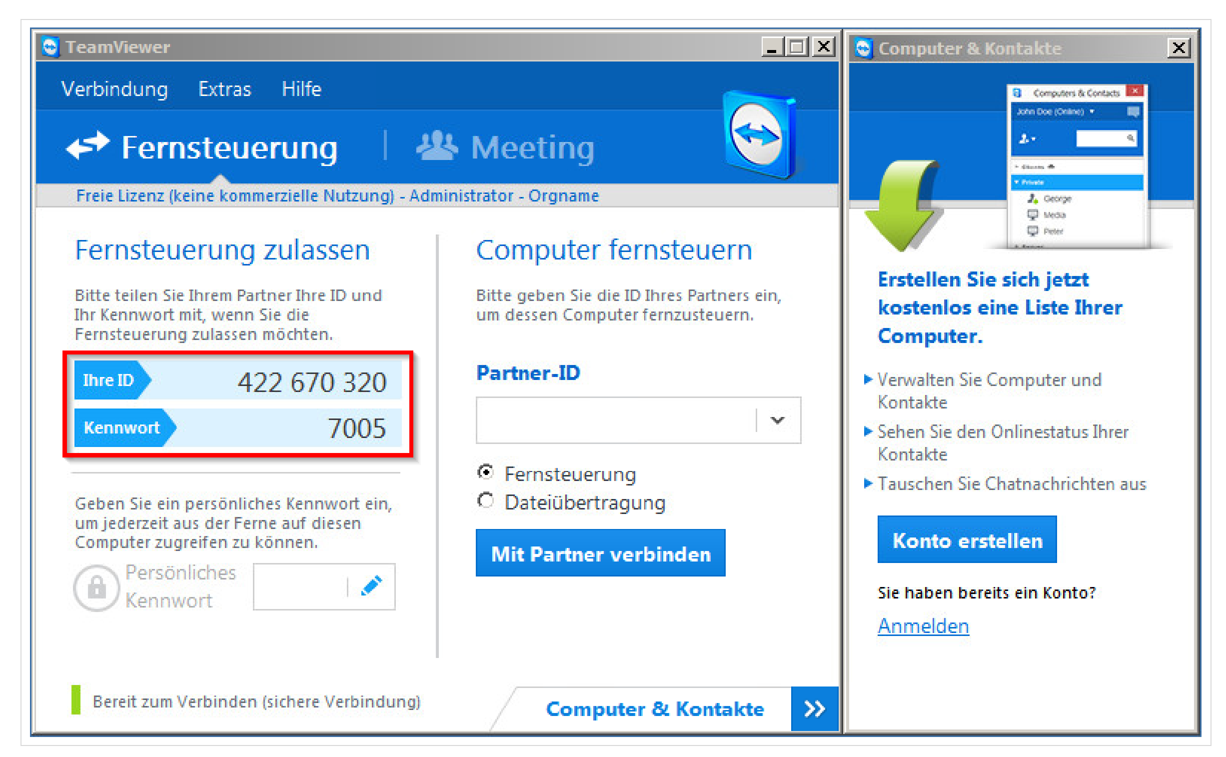


Abb. 307: Teamviewer

Es gibt zwei Optionen, wie die Hotline auf Ihren Rechner zugreift:

1. Sie müssen der Hotline jedes Mal den Zugriff gewähren, in dem Sie die ID und das tagesaktuelle Kennwort an den Hotline-Mitarbeiter übermitteln.
2. Sie richten *Teamviewer* als Systemdienst ein, der automatisch beim Systemstart des Rechners gestartet wird.



Wir empfehlen Ihnen ausdrücklich *Teamviewer* als Systemdienst zu installieren.

Dies hat den entscheidenden Vorteil, dass die Hotline jederzeit auf das System zugreifen kann selbst wenn Sie nicht vor Ort sind. Somit kann eine Fehleranalyse durch die Hotline auch in Ihrer unterrichtsfreien Zeit erfolgen.

22.2 Einrichtung von Teamviewer als Systemdienst

Damit die Hotline-Mitarbeiter jederzeit auf Ihr System zugreifen können, müssen Sie *Teamviewer* als Systemdienst mit *Windows* starten. Öffnen Sie hierfür das Menü „*Extras* | *Optionen*"

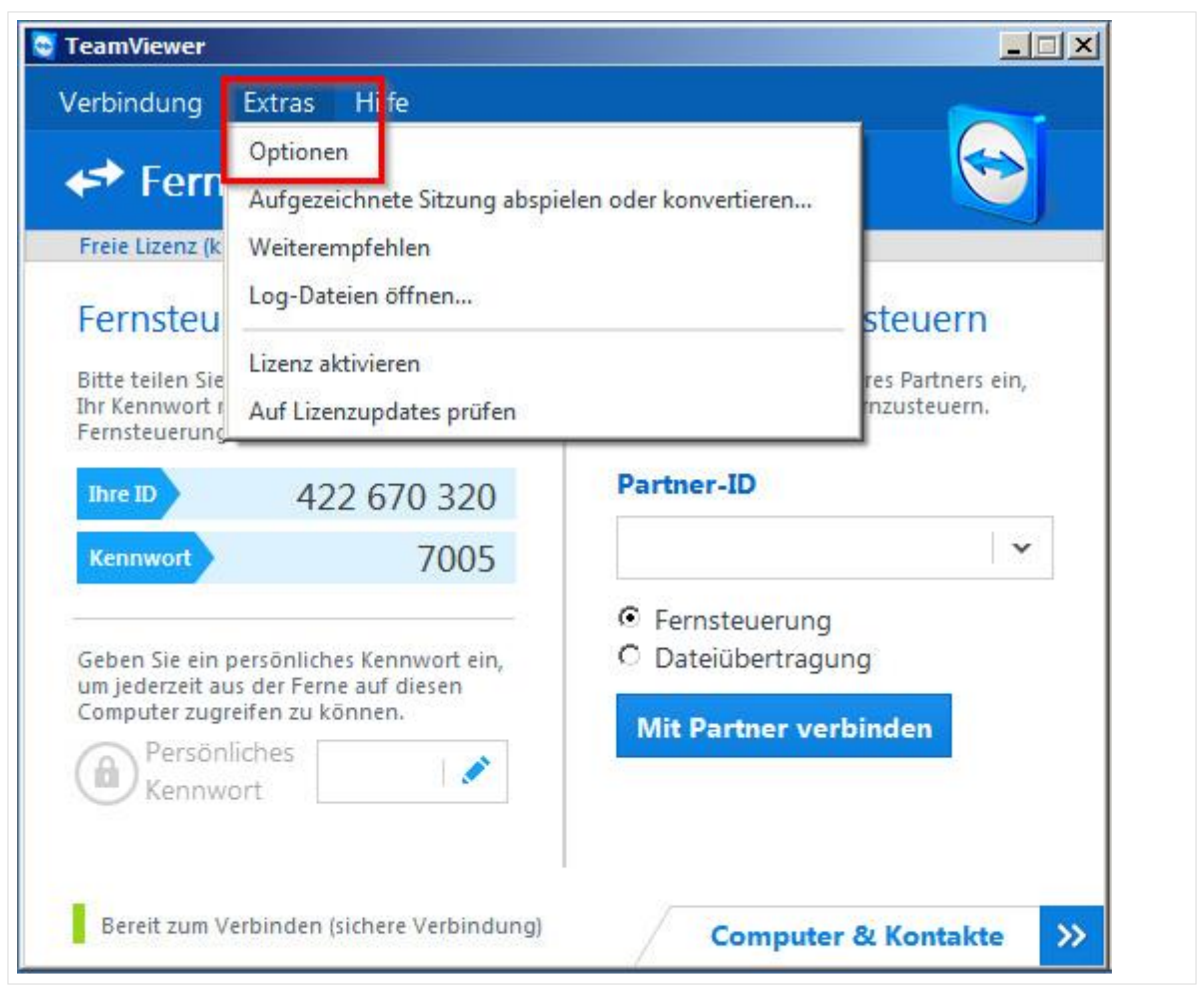


Abb. 308: Einrichtung Teamviewer als Systemdienst

Es öffnet sich ein neues Fenster mit den „*Teamviewer Einstellungen*". Im Reiter „*Allgemein*" müssen Sie die Checkbox bei „*Teamviewer mit Windows starten*" aktivieren. Es öffnet sich nochmals ein Fenster „*Permanenten Zugriff konfigurieren*", in dem Sie ein Kennwort eintragen müssen. Teilen Sie dieses Kennwort und die ID der Hotline mit.

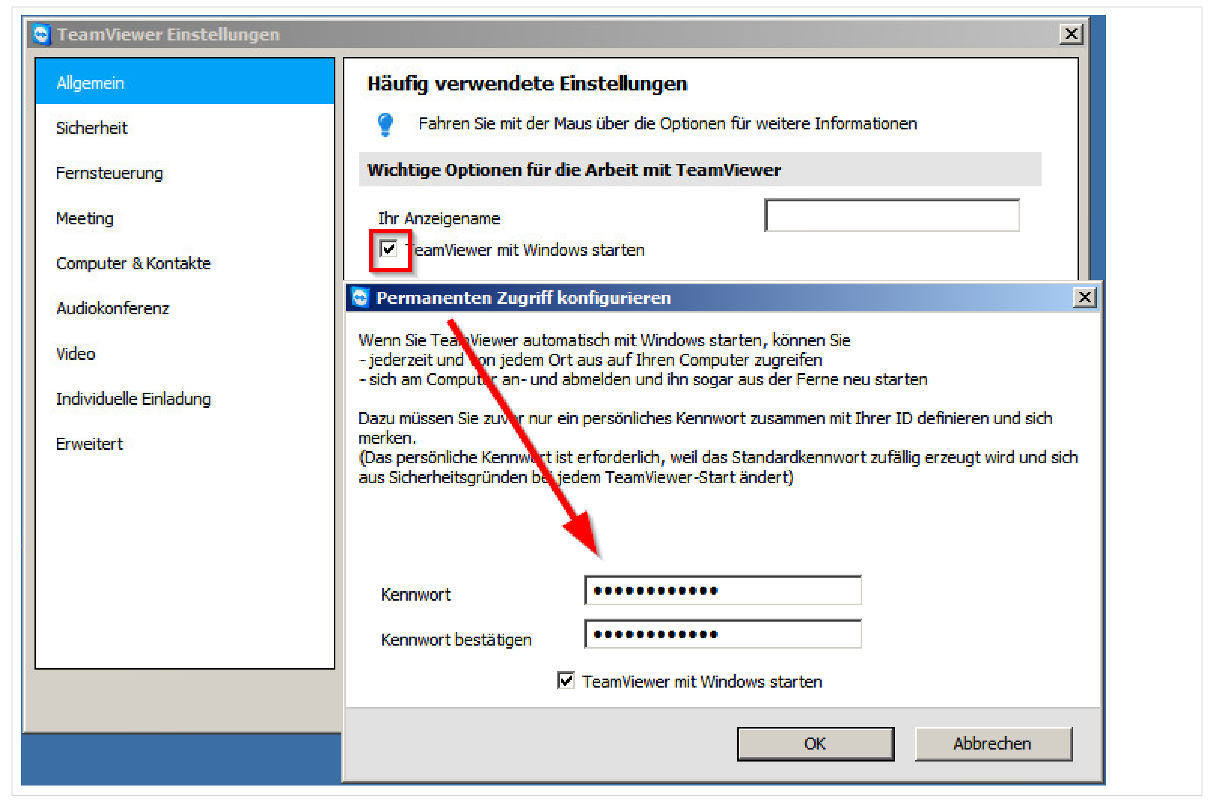


Abb. 309: Einrichtung Teamviewer als Systemdienst

23. Unterrichtzeiten



Da die Unterrichtszeiten in den Schulen variieren, ist es uns nicht möglich jede Situation vor Ort abzubilden. Im System sind vordefinierte Zeiten hinterlegt, die Sie in der *Schulkonsole* geändert werden sollten.

Die Einstellung der Unterrichtszeiten, können Sie in der Schulkonsole unter "*Schul-Administration* | *Unterrichtszeiten*" einsehen und ändern.

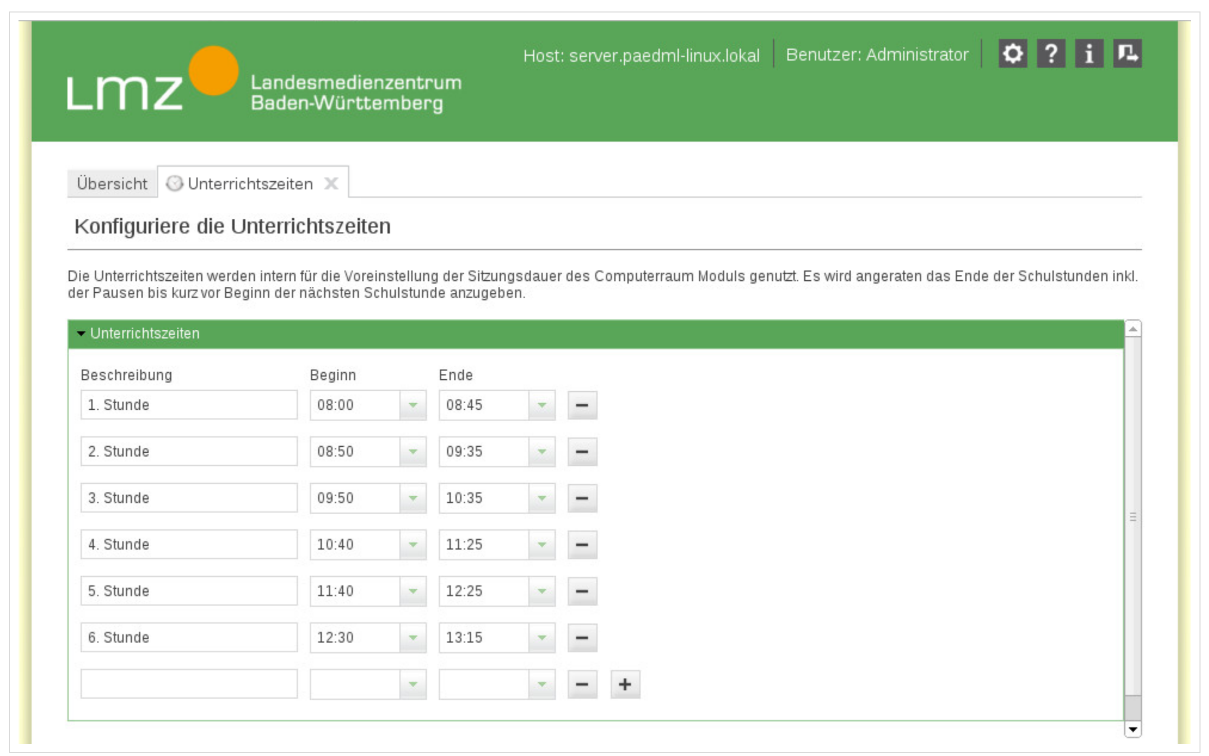


Abb. 310: Definition der Unterrichtszeiten in der Schulkonsole

Die vorgegebenen Zeiten definieren die Unterrichtszeit. Nach Ablauf einer definierten Unterrichtsstunde werden im Computerraummodul („*Unterricht* | *Computerraum*") vorgenommene Änderungen („*Benutzerdefinierte Einstellungen*") automatisch zurückgesetzt.

Der Zeitraum, in dem eigene Einstellungen im Computerraummodul aktiv sind, kann auch händisch eingestellt werden. Dadurch kann der Automatismus des Zurücksetzens auf die Standardwerte zu einer im System festgelegten Uhrzeit umgangen werden. Dies ist beispielsweise dann interessant, wenn Sie eine Doppelstunde im Computerraum unterrichten.

Sie finden diese Einstellungsmöglichkeit im Computerraummodul über den Knopf „*Einstellungen ändern*". Im obersten Feld „*Gültig bis*" können Sie eine Uhrzeit festlegen, bis zu der die Einstellungen aktiv bleiben. Anschließend können Sie die Einstellungen ändern und mit „Setzen" aktivieren".

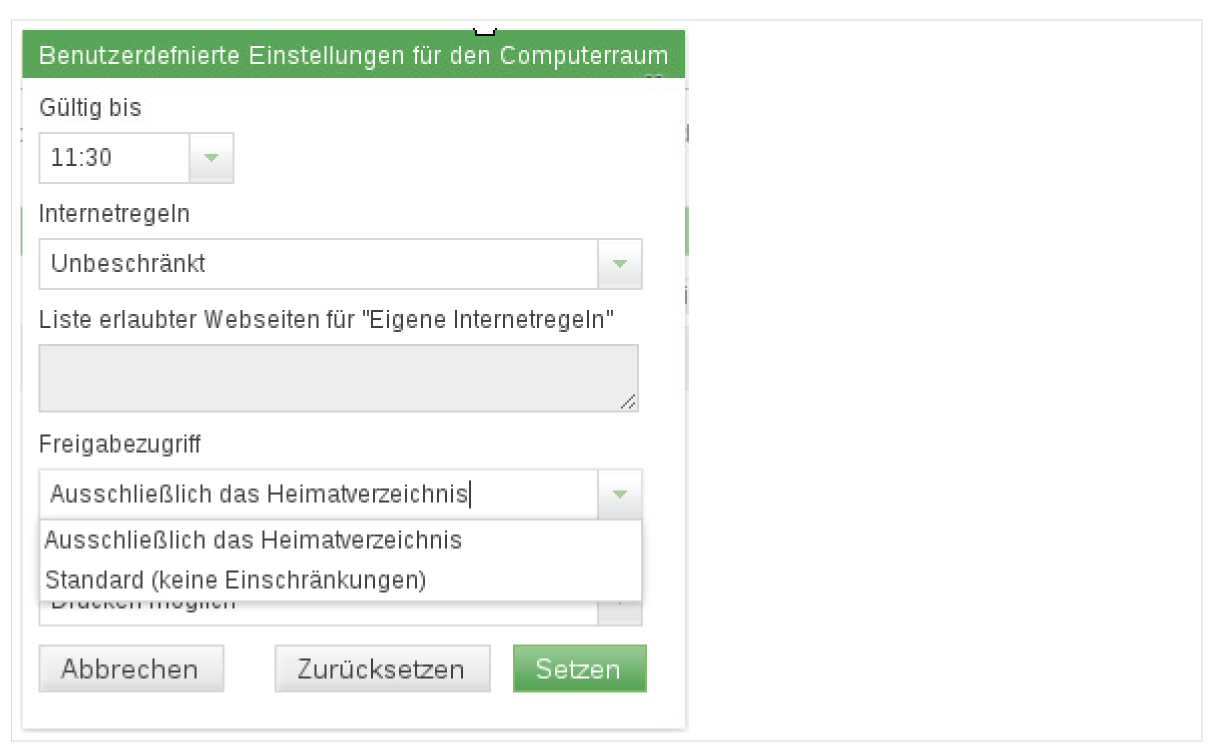


Abb. 311: Festlegen von Einstellungen für den Computerrraum

Folgende Regeln greifen bei der Arbeit in Computerräumen

1. **Internetregeln**

   Die Definition der Internetregeln geschieht über das Schulkonsolenmodul "*Schuladministration* | *Internetregeln*“. Dort werden global Regeln für den Internetzugriff definiert.

   Die Zuweisung der Regeln für Klassen/Gruppen geschieht in der Schulkonsole unter „*Schuladministration* | *Internetregeln zuweisen*".

   Computerraumregeln überschreiben die Werte für angemeldete Benutzer, sofern durch die unterrichtende Lehrkraft "*Benutzerdefinierte Einstellungen*" im Computerraummodul vorgenommen werden.

   Ein Beispiel zur Illustration:

   In einem Computerraum eines Gymnasiums ist eine AG mit Schülern der Klassen 5, 7 und der Jahrgangsstufe 2 angemeldet.

   Die Schüler der Klassen 5 und 6 dürfen im global definierten Filter nur auf die Schulhomepage zugreifen.

   Die Schüler der Klassen 7 bis 10 dürfen auf alle Seiten außer auf Facebook zugreifen.

   Die Jahrgangsstufen 1 und 2 haben unbeschränkten Zugang.

   Wenn im Computerraummodul der Wert für die Internetregeln auf „*Unbeschränkt*“ gesetzt wird, können alle Schüler auf alle Seiten zugreifen, solange sie im Computerraum angemeldet sind.

2. **Druckmodus**

Die Default-Einstellungen erlauben das Drucken in dem Raum. Der Druckerzugriff kann aber auch durch die Lehrkraft unterbunden werden (Feld: *Druckmodus*, Wert: *Drucken deaktiviert*).

3. **Freigabezugriff**

   In den Standardeinstellungen wird der Zugriff auf Freigaben („Tauschverzeichnisse") gewährt. Dieser Freigabezugriff kann aber auch beschränkt werden.

24. Known Issues

Da die *paedML Linux 6.0* eine Neuentwicklung ist und da es bei Neuentwicklungen nicht ausbleibt, dass Dinge nicht immer reibungslos funktionieren, möchten wir Sie in diesem Kapitel auf aktuelle Probleme hinweisen

24.1 Lehrertauschverzeichnis

Es kann passieren, dass Lehrer in der Festplattenübersicht unter „Computer" nicht das Lehrer-Tauschlaufwerk unter T:\ sondern ein Klassentauschlaufwerk einer Klasse, der sie zugewiesen sind, angezeigt bekommen.

Workaround:
Unterhalb der Desktop-Verknüpfung „Eigene Shares" befindet sich eine Verknüpfung zum „richtigen" Lehrer-Tauschlaufwerk.

24.2 Generieren von Benutzernamen bei CSV-Import

Benutzernamen, die über den CSV-Import erstellt werden, werden derzeit unter Umständen länger als 15 Zeichen generiert.

Bei kurzen Namen (Vorname.Nachname weniger als 15 Zeichen) tritt das Problem nicht auf (z.B. Rudi.Völler).

Zu lange Benutzernamen (z.B. Karl-Heinz.Rummenigge) führen zu Problemen beim Klassenarbeits-modus. In solchen Fällen müssen ggf. angepasste Benutzernamen verwendet werden.

24.3 Standard DHCP Lease-Zeit

Die DHCP Lease-Zeiten, also der Zeitraum, in dem eine DHCP-Adresse für ein Gerät reserviert ist, ist derzeit so eingestellt, dass neue Rechner schnell dem System hinzugefügt werden können (kurze Lease-Zeiten).

Wir empfehlen nach dem Rollout der Computerräume die DHCP Lease-Zeiten hoch zu setzen, damit die Anzahl der DHCP-Anfragen im Netz reduziert wird.

Öffnen Sie hierfür das *Schulkonsolen*-Modul "*Domäne* | *Richtlinien*".

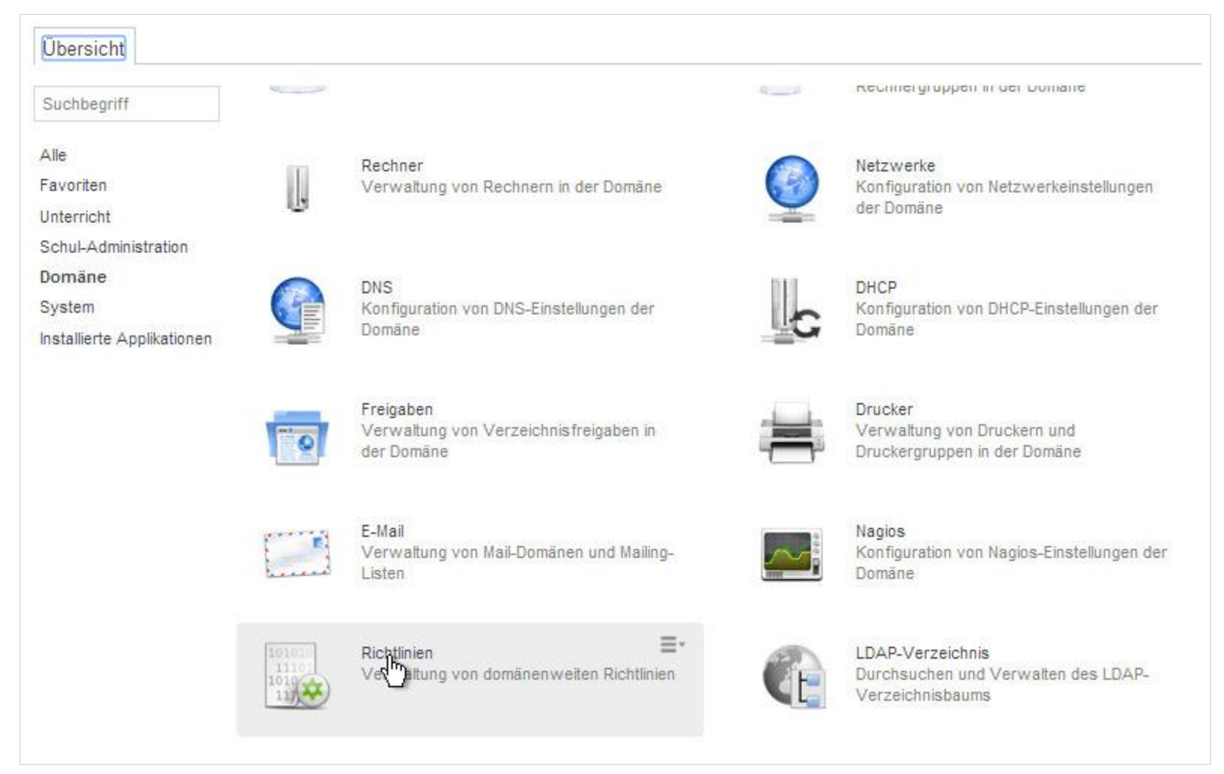


Abb. 312: Schulkonsolen-Menü: „Domäne | Richtlinien“

Öffnen Sie den Eintrag "default-settings" vom Typ "DHCP Lease Zeit" in dem Sie den Eintrag anklicken.

Name	Typ	Pfad
client-registration	DHCP Boot	lokal.paedml-linux:/policies/dhcp/boot
default-backup-umc	UMC	lokal.paedml-linux:/policies/UMC
default-central-settings	Univention Configuration Registry	lokal.paedml-linux:/policies/config-registry
default-computers-umc	UMC	lokal.paedml-linux:/policies/UMC
default-settings	UCC Benutzersitzung	lokal.paedml-linux:/policies/ucc
default-settings	DHCP DNS	lokal.paedml-linux:/policies/dhcp/dns
default-settings	DHCP Routing	lokal.paedml-linux:/policies/dhcp/routing
default-settings	DHCP Boot	lokal.paedml-linux:/policies/dhcp/boot
default-settings	Passwort	lokal.paedml-linux:/policies/users/pwhistory
default-settings	DHCP Lease-Zeit	lokal.paedml-linux:/policies/dhcp/leasetime
default-slave-umc	UMC	lokal.paedml-linux:/policies/UMC

Abb. 313: Auswahl von „default-settings DHCP Lease-Zeit“

Ändern Sie die Werte entsprechend der folgenden Tabelle ab.

Eintrag	Wert
Standard Lease-Zeit	7 Tage
Minimal Lease-Zeit	2 Stunden
Maximale Lease-Zeit	30 Tage

Tabelle 31: DHCP Lease-Zeiten

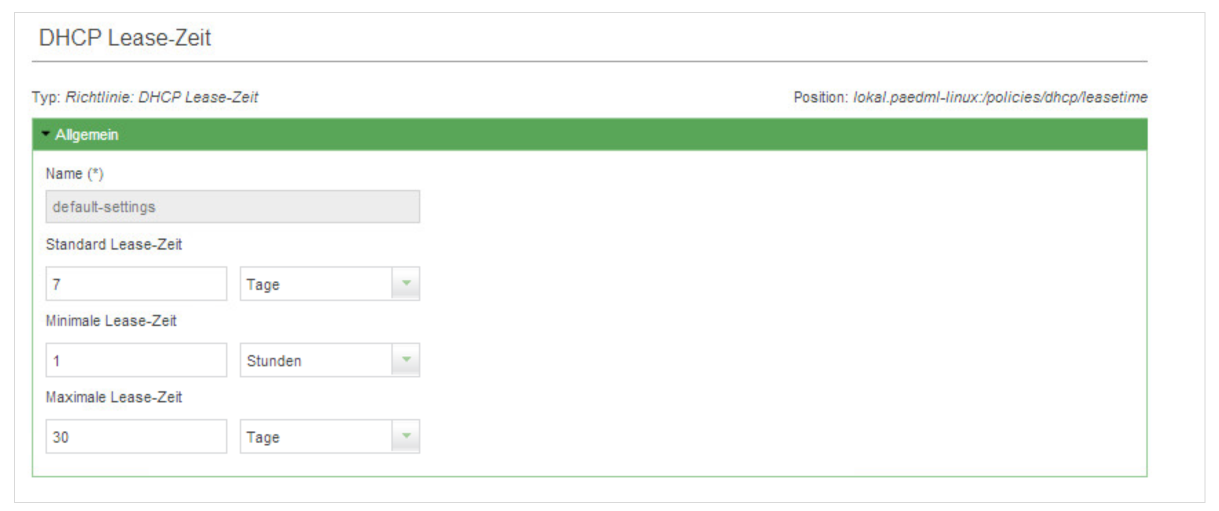


Abb. 314: Neue Lease-Zeiten

24.4 Größe von Treiberverzeichnissen bei opsi

Der Inhalt der Verzeichnisse unterhalb von "drivers/additional" auf dem opsi-Server sollte eine Gesamtgröße von 1,5 GB nicht überschreiten.

24.5 Arbeitsspeicher bei Server-VM

Die gleichzeitige Anmeldung vieler Rechner beansprucht Arbeitsspeicher auf dem Server.

Wir empfehlen bei einer Netzwerkgröße ab 30 Clients (oder zwei Computerräumen) den Arbeitsspeicher für die Server-VM auf 8 GB zu erhöhen.

24.6 Cups Error Policy

Der Druckserver Cups sollte so konfiguriert werden, dass Druckjobs im Falle eines Fehlers (zum Beispiel: kein Papier im Drucker) nicht angenommen werden.

Dies kann unter Umständen dazu führen, dass Benutzer einen Druckauftrag mehrfach absenden. Sobald der Fehler behoben ist, wird das angeforderte Dokument entsprechend mehrfach gedruckt. Wenn der Benutzer, der den Druckauftrag initiiert hat, zum Zeitpunkt der Fehlerbehebung nicht mehr im Computerraum ist, kann der Druckauftrag niemandem zugeordnet werden.

Wir empfehlen den Default-Wert der UCR-Variablen *„cups/errorpolicy“* auf *„abort-job“* zu setzen. Dadurch werden alle Druckaufträge abgebrochen, wenn der Drucker eine Fehlfunktion hat. Nachteil dieses Verfahrens ist, dass Druckaufträge im Fehlerfall nicht angenommen werden und der Benutzer den Auftrag erneut anstoßen muss.

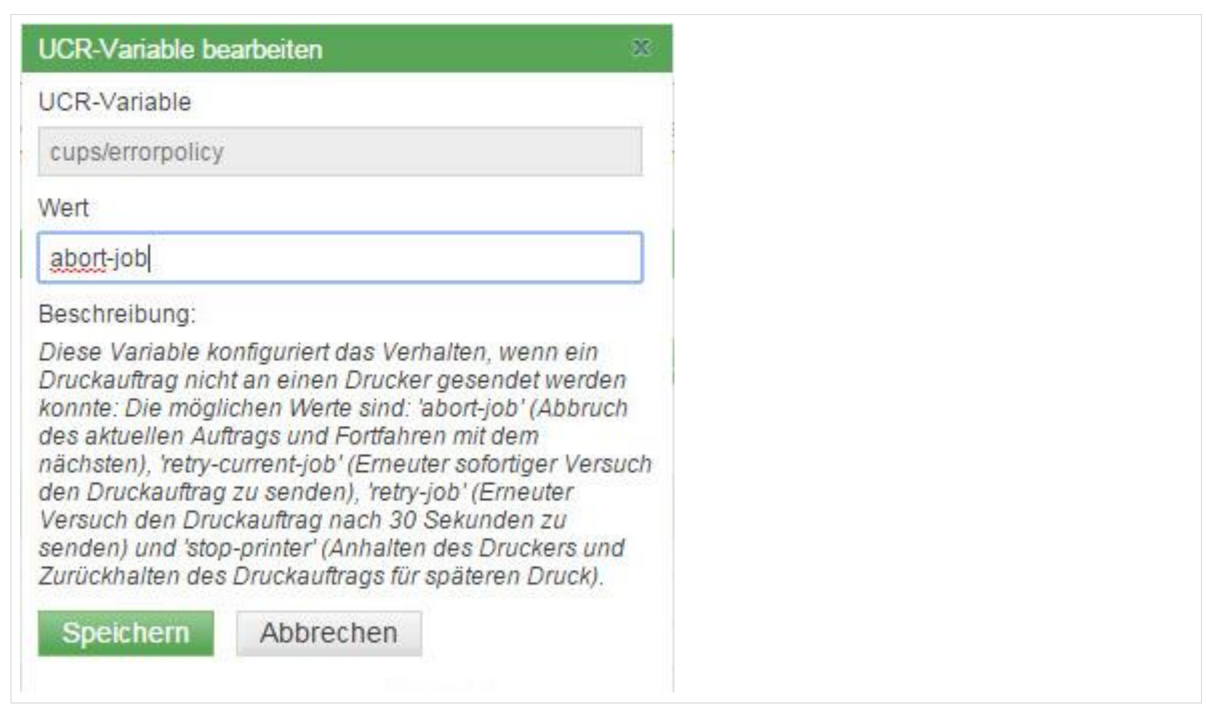


Abb. 315: Empfohlener Wert für die Cups-Fehler-Behandlung

Auf der Homepage von cups sind die folgenden Werte angegeben, die Sie in der Variable einstellen können. Bitte beachten Sie, dass jede dieser Einstellungen Vor- und Nachteile hat.

> *The following values are supported:*
>
> - ***abort-job*** *- Abort the job and proceed with the next job in the queue*
> - ***retry-current-job*** *- Retry the current job immediately*
> - ***retry-job*** *- Retry the job after waiting for N seconds; the cupsd.conf JobRetryInterval directive controls the value of N*
> - ***stop-printer*** *- Stop the printer and keep the job for future printing; this is the default value*
>
> *(Quelle: https://www.cups.org/documentation.php/doc-1.6/ref-printers-conf.html)*

Quellen

Wir haben uns bei der Erstellung dieser Dokumentation inhaltlich sowie textlich bei den folgenden Quellen bedient:

Handbuch der Firewall pfSense

- http://www.pfsense.org/index.php@option=com_content&task=view&id=50&Itemid=78.html

Dokumentationen zu opsi

- http://uib.de/www.dokus/index.html

Handbücher der Firma Univention

- http://www.univention.de/download-und-support/dokumentation/standarddokumentation/

weiterführende Adressen zur paedML Linux

Startseite Landesmedienzentrum Baden-Württemberg

- http://www.lmz-bw.de/

Startseite Support-Netz

- http://www.lmz-bw.de/technische-unterstuetzung/kundenportal/linux.html

Anleitungen für die paedML Linux

- http://www.lmz-bw.de/technische-unterstuetzung/kundenportal/linux/dokumentationen.html

Beratungsangebote rund um die paedML

- http://www.lmz-bw.de/technische-unterstuetzung/beratung.html

Multimedia-Empfehlungen

- http://www.lmz-bw.de/technische-unterstuetzung/beratung/infothek/-materialien/medienentwicklungsplan/multimedia-empfehlungen.html

Fortbildungen zur paedML

- http://lehrerfortbildung-bw.de/

Third-Party-Software der paedML Linux

BackupPC

- http://backuppc.sourceforge.net/

horde

- http://www.horde.org/

Nagios

- http://www.nagios.org/

OpenVPN

- www.openvpn.net

opsi

- www.uib.de

shalla-Liste

- www.shallalist.de/

Univention

- www.univention.de

VMware

- www.vmware.com

Glossar

- **AdminVM** – Rechner für administrative Aufgaben
- **BackupPC** – Software, mit der die Server der *paedML Linux* gesichert werden können
- **Backup-Server** – auch „**opsi-Server**“; System auf dem der Dienst *opsi* installiert ist, über den Software und Betriebssystem installiert werden können
- **Gäste-Netz** – Netzwerk für schulfremde Geräte
- **horde** – Groupwarelösung für den internen Mailversand
- **Hypervisor** – Virtualisierungs-Software; minimales Betriebssystem, das die Container für die Virtualisierung bereitstellt.
- **localboot-produkt** – Bezeichnung für Programme, die auf laufenden Rechner via *opsi* ausgespielt werden können.
- **Management Netzwerk** – Netzwerk, aus dem Zugriff auf den Hypervisor umgesetzt wird (im Auslieferungszustand das pädagogische Netz).
- **nagios** – Software zur Überwachung von Systemdiensten und Zustand der *paedML Server*
- **netboot-produkt** – Bezeichnung für *opsi*-Routinen, die beim Systemstart eines Rechners ausgeführt werden (z.B. Betriebssysteminstallation, Backup, Restore,...)
- **opsi** – „Open PC Server Integration“, das Client-Management-System, über das in der *paedML* Software und Betriebssysteminstallationen verteilt werden.
- **opsi-configed** – grafisches Benutzerinterface für *opsi*
- **ospi-depot** – Zentraler Ablageort für *opsi*-Programmdateien
- **pfSense** – Firewall-Lösung, die in der *paedML Linux* zum Einsatz kommt
- **Schulkonsole** – Verwaltungsoberfläche für administrative Aufgaben der *paedML Linux*
- **Server** – auch „**Master-Server**“ der *paedML Linux* mit Home-Verzeichnissen der Benutzter, LDAP-Verzeichnisbaum,…
- **Virtualisierungshost** – Server, auf dem der Hypervisor installiert ist
- **Vmware ESX(i)** – Hypervisor auf dem die Virtualisierung läuft.
- **vSphere Client** – Software zur Verwaltung virtueller Maschinen von *VMware*

Anhang A Nomenklatur



1. Bitte beachten Sie unbedingt, dass die Vergabe von Sonderzeichen in Namen oder Passwörtern zu Problemen führen kann. Bitte beachten Sie außerdem, dass wir vom Umbenennen von Benutzern, Geräten, Räumen, Projekten ausdrücklich abraten. Bitte löschen Sie stattdessen das entsprechende Objekt[68] und legen Sie es neu an.
2. Achten Sie beim Import von Listen (Benutzerlisten/Gerätelisten) auf die richtige Zeichencodierung[69] (Character Encoding) der Dateien.

   Unterstützt wird nur der Zeichensatz ANSI. Bei anderen Zeichensätzen kann es zu Problemen beim Import von Daten kommen.
3. Die Namen aller „Objekte“ (Geräte sowie Benutzer), die im Server angelegt werden, müssen eindeutig sein. So darf beispielsweise ein Laptop des Kollegen Netzwerkberaters nicht als Computer „Netzwerkberater“ angelegt werden.
4. „Case sensitivity“[70], also die Unterscheidung von Groß- und Kleinbuchstaben ist ein wichtiges Thema in Linux. Ein Objekt PC01 ist unter Umständen nicht dasselbe wie das Objekt pc01.

   Eine Möglichkeit, dieses Problem zu umgehen, ist die konsequente Kleinschreibung aller Namen für Objekte, die Sie in der paedML anlegen (Benutzernamen, Klassenräume, Geräte,…).

Global sind die folgenden Zeichen erlaubt:
Großbuchstaben, Kleinbuchstaben, - (Bindestrich), _ (Unterstrich – **außer in Geräte- und Raumnamen**), Leerzeichen und Ziffern. Bitte vermeiden Sie Sonderzeichen (zum Beispiel Umlaute (ä, ö, ü), scharfes S (ß), Akzente (é, è,…) und Satzzeichen in Benutzer- und Objektnamen.

Objekte	Hinweise
Benutzernamen	▪ Umlaute und das scharfe S (ß) werden beim Import von Benutzern vom System verarbeitet. ▪ Achten Sie darauf, dass keine Sonderzeichen (?, !,…) Accents oder ähnliches in den Benutzernamen vorkommen dürfen. ▪ Die Zeichenlänge von Benutzernamen sollte auf 15 Zeichen beschränkt werden, sofern Sie den Klassenarbeitsmodus nutzen wollen. Hierfür müssen der Import-Liste Benutzernamen mitgegeben werden.

[68] Alternativ empfehlen wir zu überlegen, ob eine Änderung überhaupt notwendig ist. Wenn sich bspw. der Nachname eines Benutzers ändert, dann kann dieser unter Umständen auch mit dem alten Namen im System geführt werden. Zum Thema Daten gelöschter Benutzer beachten Sie bitte die Hinweise in Kapitel 3.5.1 auf Seite 39.

[69] http://de.wikipedia.org/wiki/Zeichenkodierung

[70] http://de.wikipedia.org/wiki/Case_sensitivity

Rechner- und Gerätenamen	▪	Die Länge von Gerätenamen darf 16 Zeichen nicht überschreiten!
	▪	**Vorsicht:** In Rechner- und Gerätenamen dürfen keine Unterstriche verwendet werden. Der Unterstrich wird zwar von der Schulkonsole akzeptiert, die Rechner/Räume werden dann allerdings nicht nach opsi synchronisiert!
Arbeitsgruppen	▪	Hier sind keine Sonderzeichen oder Umlaute erlaubt.
Imagenamen	▪	Hier sind keine Unterstriche erlaubt.
Raumbezeichnungen	▪	s. Rechner- und Gerätenamen

Tabelle 32: Besonderheiten bei Namen von Objekten

Feldtrenner für Import-Listen

Benutzer und Geräte können via Listenimport eingepflegt werden (Vgl. Kapitel 3.1, Seite 42 und Kapitel 4.2.1, Seite 68). Das Skript für den Benutzerimport richtet sich nach den Vorgaben der Vorgänger-Versionen der *paedML Linux*, das Skript für den Geräteimport ist ein Skript der Firma *Univention*, das wir in die *paedML Linux* übernommen haben.

Die Trennzeichen dieser Listentypen sind aufgrund ihrer Herkunft unterschiedlich. Dies gilt es beim Listenimport zu beachten.

Liste	Trennzeichen	
Benutzerliste	▪	; Zwischen den einzelnen Feldern steht ein **Semikolon als Trennzeichen**.
	▪	Am Ende jedes Datensatzes sollte kein abschließendes Trennzeichen gesetzt werden.
	▪	In den Datenfeldern dürfen keine Extra-Leerzeichen oder Extra-Tabulatoren vorhanden sein
Geräteliste	▪	→ Zwischen den einzelnen Feldern steht ein **Tabulator als Trennzeichen**.

Tabelle 33: Trennzeichen bei Listenimport

Einträge von opsi-Werten



Alle opsi-Felder dürfen **KEINE SONDERZEICHEN, KEINE UMLAUTE UND KEINE LEERZEICHEN** beinhalten. Erlaubt ist der Bindestrich (-) und der Unterstrich (_).

Anhang B Firewallkonfiguration

Alle hier beschriebenen Funktionen können Sie über das Webinterface der *pfSense* Firewall konfigurieren. **Die Konfiguration der Firewall sollte ausschließlich über dieses Webinterface erfolgen.**

Sie können die Startseite der *pfSense* Firewall unter der Adresse https://firewall.paedml-linux.lokal erreichen.



Die Konfiguration der Firewall ist mit Absicht nicht en Detail beschrieben.

Anpassungen an der pfSense-Firewall sollten für den Normalbetrieb der paedML Linux nicht notwendig sein. Die Standardwerte der Firewall-Konfiguration sollten nach Möglichkeit nicht geändert werden.

Änderungen in der Firewall können Auswirkungen in Puncto Sicherheit des schulischen Netzwerkes oder der auf Funktionen der *paedML Linux* haben.

Nehmen Sie Modifikationen an der Firewall nur dann vor, wenn Sie sich im Klaren darüber sind, was die von Ihnen getätigten Änderungen bewirken.

Dokumentieren Sie alle Änderungen, damit im Fehlerfall der Standard wieder hergestellt werden kann.

B.1 Firewall-Regeln

In den Firewall-Regeln wird festgelegt, wie sich verschiedene Netzwerke – in unserem Fall das Internet, das pädagogische Netz, das Gäste-Netz und das OpenVPN-Netz (über das externe Geräte mit dem Schulnetz verbunden werden können) – zueinander verhalten.

Die an der Firewall angeschlossenen Netzwerke bekommen über definierte Regelsätze Zugriff auf Netzwerkdienste (z.B. HTTP, Mail-Dienste). Über diese Einstellungen kann aber ein Zugriff auch gezielt unterbunden werden.



Aus Darstellungsgründen wurden die Inhalte der hier wieder gegebenen pfSense-Tabellen umstrukturiert.

Die erste Spalte kennzeichnet den Regelstatus.

Das Beschreibungsfeld wurde von ganz hinten an die zweite Position geholt.

Auf die Felder „Queue[71]“ und „Schedule[72]“ wurde in den folgenden Darstellungen verzichtet, da Sie in der paedML Linux nicht zum Einsatz kommen.

[71] Hiermit könnte Traffic-Shaping definiert werden.

[72] Hierüber könnte definiert werden, ob Firewall-Regeln nur zu bestimmten Zeiten gelten.

Internet: https://firewall.paedml-linux.lokal/firewall_rules.php?if=wan

Regelstatus	Description/ Beschreibung	Proto(koll)	Quelle (Source)	(Quell) Ports	Ziel (Destination)	(Ziel)Ports	Gateway
Block	Block Private Networks	*	RFC 1918 networks	*	*	*	*
Block	Block logon networks	*	Reserved/ not assigned by IANA	*	*	*	*
Reject	Verbiete Zugriff auf externe Mailserver (SMTP)	IPv4 TCP	*	*	*	25 (SMTP)	*
Pass	OpenVPN INTERNET	IPv4 UDP	*	*	INTERNET address	1194 (OpenVPN)	*

Tabelle 34: Firewall-Regeln Internet

Pädagogisches Netz: https://firewall.paedml-linux.lokal/firewall_rules.php?if=lan

Regelstatus	Description/ Beschreibung	Proto(koll)	Quelle (Source)	(Quell) Ports	Ziel (Destination)	(Ziel)Port	Gateway
Pass	Anti-Lockout Rule	*	*	*	PAEDAGOGIK address	443 / 80	*
Pass	Erlaube ICMP-Anfragen von PAEDAGOGIK in alle Netze	IPv4 ICMP	PAEDAGOGIK net	*	*	*	*
Reject	Verbiete Zugriff auf externe Mailserver (SMTP)	IPv4 ICMP	*	*	*	25 (SMTP)	*
Pass	Erlaube direkten Internet-Zugriff für „server“	IPv4 *	10.1.0.1	*	*	*	*
Pass	Erlaube direkten Internet-Zugriff für „backup“	IPv4 *	10.1.0.2	*	*	*	*
Pass	Erlaube direkten Internet-Zugriff für	IPv4 *	10.1.0.13	*	*	*	*

	„AdminVM“						
Pass (deaktiviert)	Eralube direkten Internetzugriff NUR für Server	IPv4 *	10.1.0.0/27	*	*	*	*
Reject	Verbiete direkten Internetzugriff für nicht-Server	IPv4 *	*	*	*	*	*

Tabelle 35: Firewall-Regeln pädagogisches Netz

Gäste-Netz: https://firewall.paedml-linux.lokal/firewall_rules.php?if=opt1

Regelstatus	Description/ Beschreibung	Proto(koll)	Quelle (Source)	(Quell) Ports	Ziel (Destination)	(Ziel)Ports	Gateway
Pass	OpenVPN Gäste	IPv4 UDP	GAESTE net	*	GAESTE address	1194 (openVPN)	*
Pass	Erlaube ICMP	IPv4 ICMP	*	*	*	*	*
Pass	Erlaube DNS-Zugriff	IPv4 UDP	GAESTE net	*	GAESTE address	53 (DNS)	*
Pass	Erlaube NTP-Zugriff	IPv4 UDP	GAESTE net	*	GAESTE address	123 (NTP)	*
Pass (deaktiviert)	Erlaube Captive Portal Zugriff	IPv4 TCP	GAESTE net	*	GAESTE address	8000	*
Pass	NAT Proxy-Zugriff aus Gäste-Netz erlaubt	IPv4 TCP	*	*	10.1.0.1	3128	*
Pass (deaktiviert)	NAT RADIUS-Zugriff	IPv4 TCP/UDP	*	*	10.1.0.1	1812 - 1813	*
Reject	Verbieten allen weiteren Zugriff auf pfSense	IPv4 *	*	*	GAESTE address	*	*
Pass (deaktiviert)	Erlaube sämtliche weitere Zugriff über Captive Portal	IPv4 *	GAESTE net	*	nicht aus PAEDAGOGIK net	*	*
Reject	Verbiete alle anderen Zugriff	*	*	*	*	*	*

Tabelle 36: Firewall-Regeln Gäste-Netz

OpenVPN-Netz: https://firewall.paedml-linux.lokal/firewall_rules.php?if=openvpn

Regelstatus	Description/ Beschreibung	Proto(koll)	Quelle (Source)	(Quell) Ports	Ziel (Destination)	(Ziel)Ports	Gateway
Pass	OpenVPN	IPv4 *	*	*	PAEDAGOGIK net	*	*

Tabelle 37: Firewall-Regeln OpenVPN

B.2 NAT-Regeln

Über NAT(Network Address Translation)-Regeln wird der Zugriff auf Geräte innerhalb eines Netzwerkes gesteuert. Im Fall der paedML Linux steht die pfSense Firewall als Verbindungsglied zwischen Intranet und dem schulischen Netzwerk. In NAT-Regeln können Geräte für externen Zugriff über das Internet frei geschaltet werden. Dies wird zum Beispiel genutzt, um den ssh-Fernwartungszugriff auf Rechner im Schulnetz frei zu geben.

Port-Forwarding: https://firewall.paedml-linux.lokal/firewall_nat.php

Regelstatus	Description/ Beschreibung	If (Interface, über das Verbindung aufgebaut wird)	Proto(koll)	Quell-Adresse (Src. Addr.)	Quell-Ports (Src. Ports)	Ziel-Adresse (Dest. Addr.)	
Pass (deaktiviert)	SSH-Zugriff auf Server	INTERNET	TCP	*	*	INTERNET address	(1---)
Pass (deaktiviert)	SSH-Zugriff auf Backup-Server	INTERNET	TCP	*	*	INTERNET address	(2---)
Pass (deaktiviert)	HTTPS-Zugriff auf 10.1.0.5 (optionaler Web-Server)	INTERNET	TCP	*	*	INTERNET address	(3---)
Linked Rule[73]	Proxyzugriff aus Gäste-Netz erlaubt	GAESTE	TCP	*	*	GAESTE address	(4---)
Linked Rule	RADIUS-Zugriff aus GAESTE-	GAESTE	TCP/ UDP	*	*	10.1.0.1	(5---)

[73] „Linked Rules“ sind NAT-Regeln, die mit Firewallregeln verknüpft sind (z.B. Verknüpfung "Proxyzugriff aus Gäste-Netz erlaubt" ist verknüpft mit NAT-Regel Proxyzugriff aus Gäste-Netz erlaubt"

Netz erlauben

Tabelle 38: NAT-Regeln Anfang…

	Ziel-Ports (Dest. Ports)	Description/ Beschreibung	NAT IP	NAT Ports
(---1)	22222	SSH-Zugriff auf Server	10.1.0.1	22 (SSH)
(---2)	22223	SSH-Zugriff auf Backup-Server	10.1.0.2	22 (SSH)
(---3)	443	HTTPS-Zugriff auf 10.1.0.5 (optionaler Web-Server)	10.1.0.5	443 (HTTPS)
(---4)	3128	Proxyzugriff aus Gäste-Netz erlaubt	10.1.0.1	3128
(---5)	1812 - 1813	RADIUS-Zugriff aus GAESTE-Netz erlauben	10.1.0.1	1812 - 1813

Tabelle 39: … NAT-Regeln Fortsetzung

B.3 Anpassungen an der Firewall

B.3.1 Zugriff von außen

https://firewall.paedml-linux.lokal | Firewall | NAT
Mittels der *Network Address Translation* (*NAT*) können Anfragen von außen (Internet) gezielt auf Geräte im Intranet weiter geleitet werden. NAT-Regeln öffnen gezielt „Fenster" nach außen, über die ein Zugriff erfolgen kann. **ACHTUNG! Über offene Ports können unter Umständen auch unberechtigte Personen Zugriff auf Ihr Netzwerk erhalten. Eine Absicherung der erreichbaren Dienste (zum Beispiel über sichere Passwörter) sollte daher durchgeführt werden.**

Im System sind Regeln für den Zugriff auf Server und *Backup-Server* via SSH und den Zugriff auf den optionalen Webserver via HTTPS vorkonfiguriert. Damit diese Regeln aktiv werden, müssen Sie bearbeitet und aktiviert werden. (Auslieferungszustand der drei Regeln ist „*disabled*")

Des Weiteren gibt es eine Regel für das Gäste-Netz, die den Zugriff über den Webproxy herstellt. Dadurch können Geräte aus dem Gäste-Netz auf das Internet zugreifen. Dieser Zugriff geschieht über den Proxy der paedML Linux und somit über den Jugendschutzfilter.

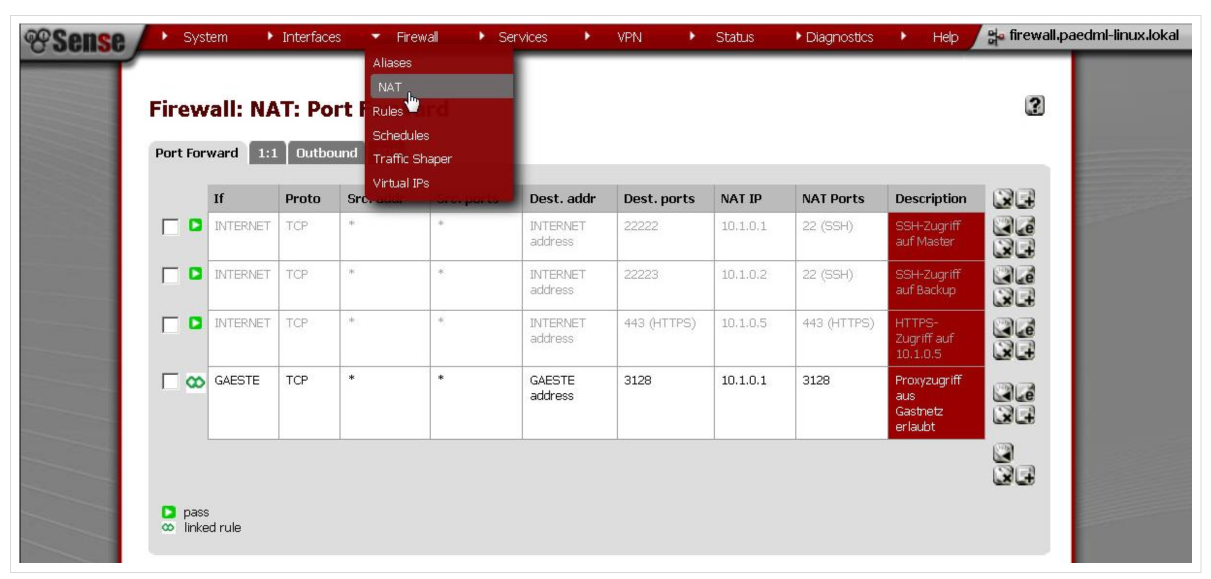


Abb. 316: NAT in der paedML Linux.

B.3.2 Zugriff nach außen

https://firewall.paedml-linux.lokal | Firewall | Rules

Die Firewallregeln definieren, wie nach außen zugegriffen werden kann. Konkret bedeutet das, dass nicht alle Rechner im Intranet auf externe Dienste zugreifen können. Die Firewallregeln werden pro Netzwerk der Firewall (Internet, pädagogisches Netz, Gäste-Netz, OpenVPN-Netz) definiert.

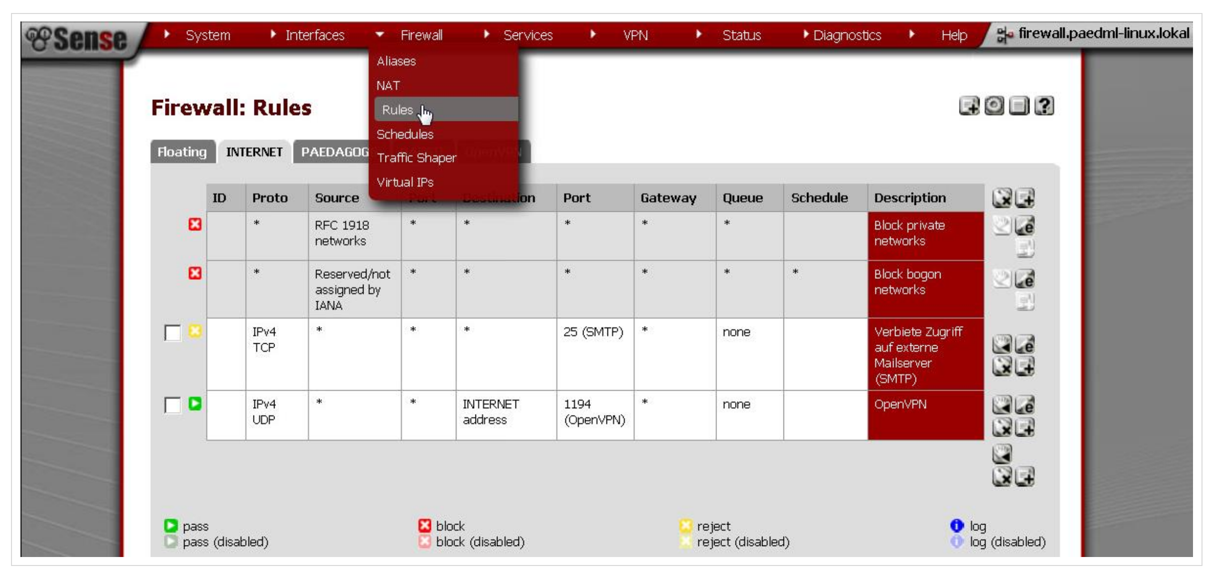


Abb. 317: Zugriff auf externe Dienste

B.3.3 Änderungen des Zeitservers

Je nach Provider muss ggf. der Zeitserver in der pfSense von de.pool.ntp.org geändert werden.

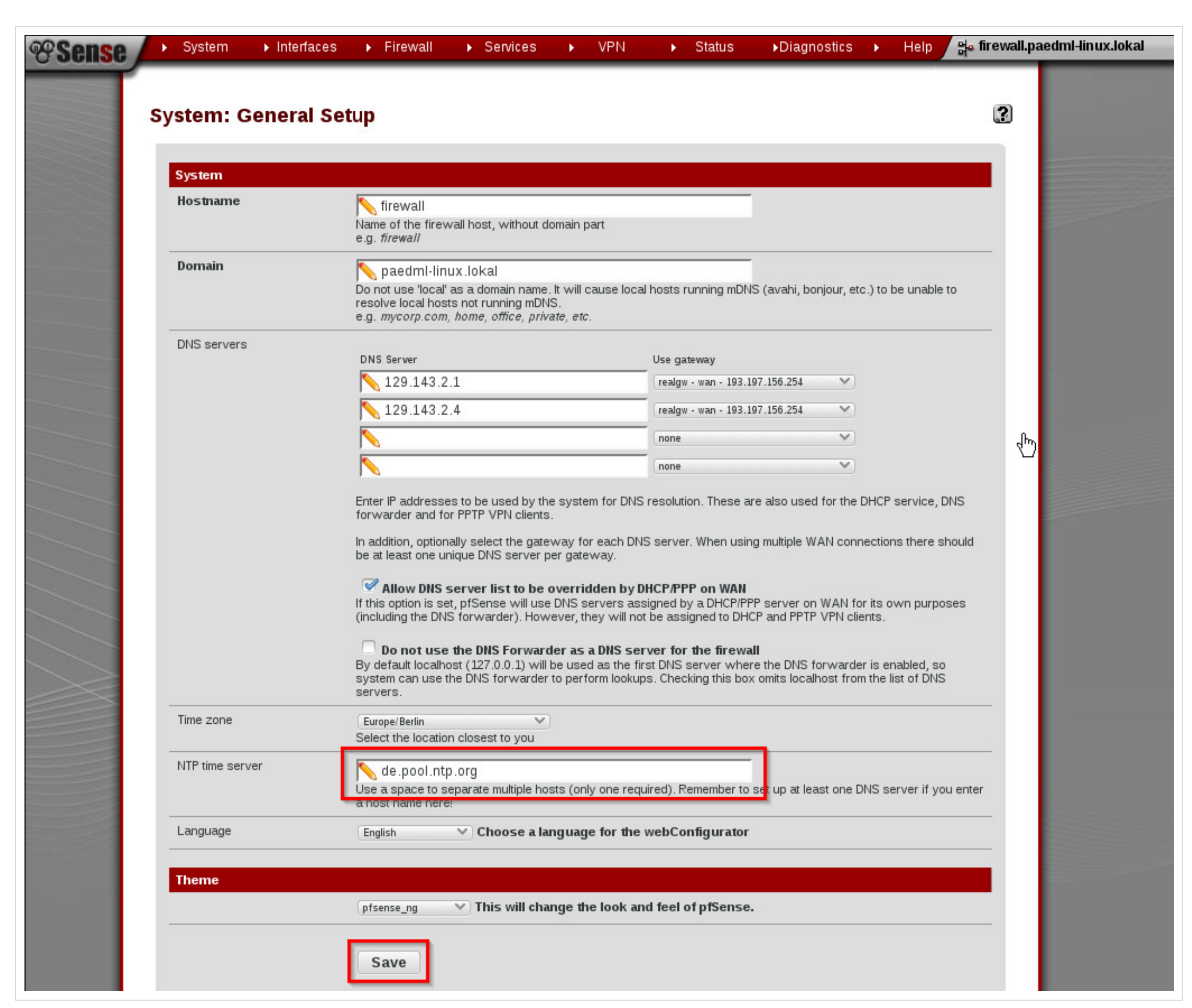


Abb. 318: Eintragen eines neuen Zeitservers.

Anhang C Materialverteilung – Dateigröße

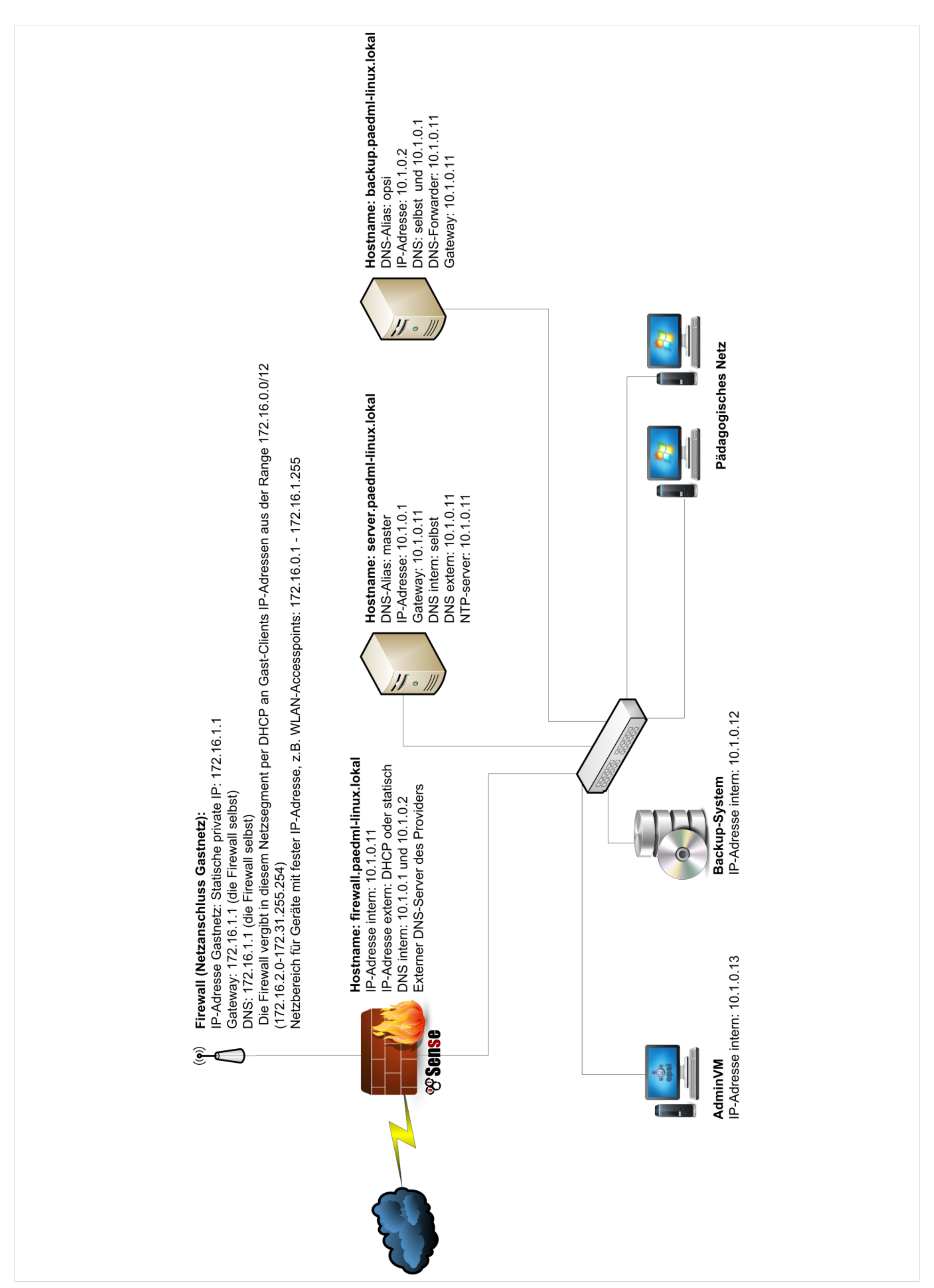
Beim Verteilen von Material über die Schulkonsole ist eine Größenbeschränkung aktiv. Diese verhindert, dass zu große Dateien verteilt werden.

In der UCR-Variable „*umc/server/upload/max*“ kann dieser Wert bei Bedarf angepasst werden.

Im Auslieferungszustand ist der Wert auf 512MB gesetzt ((512*1024=524288). Der Wert wird in Kilobyte in die UCR-Variable eingetragen. Pro MegaByte sind 1024 KiloByte.

Die Formel zur Berechnung von n MB lautet daher `n*1024`. Der errechnete Wert ist in die Variable einzutragen.

Anhang D Grafiken



Anhang 1: Übersicht über die Rechner der paedML Linux

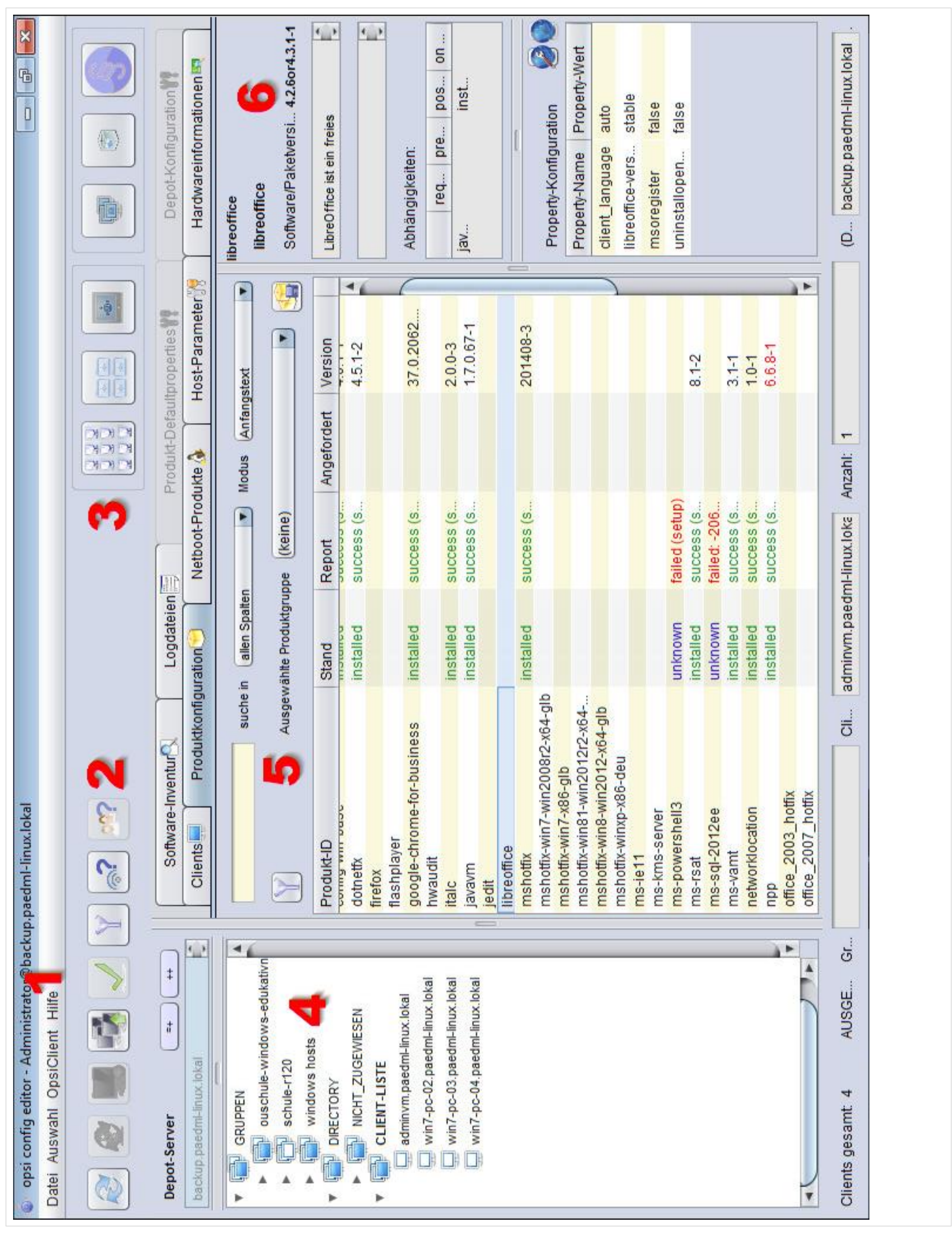


Abb. 319: opsi-Konsole

Anhang E Übersicht über opsi-Images

Datum	*Imagename*	*Rechner/ Gruppe*	*Bemerkungen*

Tabelle 40 - Vorlage für Dokumentation von opsi-Images

Landesmedienzentrum Baden-Württemberg (LMZ)
Support Netz
Rotenbergstraße 111

70190 Stuttgart



